Manual 3060 System

State of: July 2007

If the contents of the foreign language version of the documentation differ from the contents of the original German version, the original German version shall apply in case of doubt. We reserve the right to make technical changes.

SimonsVoss Technologies AG • Feringastraße 4 • 85774 Unterföhring • Germany
Hotline 01805-SV3060 • FAQs www.simons-voss.de
Telefon +49-89-99 228-0 • Fax +49-89-99 228-222

SimonsVoss technologies

Table of Contents

Version: March 2008

SimonsVoss technologies

Table of Contents

P **PEOPLE TO CONTACT**
Sales
Technical
Address in Munich

D **DIGITAL LOCKING SYSTEM 3060**
General method of operation
The components
Access control, time zone administration

T **TRANSPONDER 3064**
Method of operation
Loss of a transponder
Password-protected transponder

Q **BIOMETRIC TRANSPONDER Q3007**
Method of operation
Learn-mode
Recognize-mode
Deleate-mode

BIOMETRIC READER Q3008
Method of operation
Learn-mode
Recognize-mode
Deleate-mode

PINCODE-KEYPAD 3068
Method of operation
Initiation
Programming
Battery warning

V **DIGITAL LOCKING CYLINDER 3061 VDS (TN3)**
Method of operation
Installation instructions
Battery warning, battery replacement

Table of Contents

DIGITAL LOCKING CYLINDER 3061 (TN4)
Method of operation
Installation instructions
Battery warning, battery replacement

H

DIGITAL HALF CYLINDER 3061 (TN3)
Method of operation
Installation instructions
Battery warning, battery replacement

DIGITAL HALF CYLINDER 3061 (TN4)
Method of operation
Installation instructions
Battery warning, battery replacement

R

DIGITAL SMART RELAY 3063
Installation
Connections
Programming

SMART OUTPUT MODULE
Installation
Connections
Programming

SHUNT LOCK FUNCTION 3066
Activation unit
Deactivation unit
Installation and connecting plan

E

SHUNT LOCK FUNCTION 3066 VDS
Master activation unit
Slave activation unit
Deactivation unit
VdS-compliant installation

Table of Contents

WAVENET RADIO NETWORK
Components
Structure
Installation

N

LON NETWORK 3065
Network configuration
Components
Installation

M

PROGRAMMING TRANSPONDER 3067
Backup card
Error messages
Programming

P

PALM CD2
Initiation
Export and import
Programming

SMART CD
Initiation
Export and import
Programming +65

K

KEY
Explanation of technical terms
Special Symbols

People to contact

Version: September 2006

SimonsVoss technologies

People to contact

SALES
If you have any questions please contact our specialist dealers, or the sales representative responsible for your region. You can obtain information concerning the responsible contact at the following telephone number.

+49 89-9 92 28-180

United Kingdom
SimonsVoss Technologies Ltd.
Mr. Oliver Quaisser
44 Newton Court, Old Windsor
Berkshire SL4 2SN
Great Britain
Tel. +44 / (0)1753 / 85 98 44
Fax +44 / (0)1753 / 83 17 03
Email: oliver.quaisser@simons-voss.co.uk

Singapore and Asia
SimonsVoss Security Technologies (Asia) Pte. Ltd.
Mr. Jason P. Kurek
72 B Pagoda Street
Republic of Singapore 059231
Tel. (65) 6227 7318
Fax (65) 6227 7018
Email: jpk@simonsvossasia.com

Middle East
SimonsVoss Technologies (Middle East) FZ-LCC
Dubai Internet City
P.O. Box 500188
Dubai, UAE
Tel. +9714 3629761
E-Mail: uae@simons-voss.com

Headquaters Munich
SimonsVoss Technologies AG
Feringastraße 4
85774 Unterföhring
Germany

Tel: +49 89-9 92 28-180
Fax +49 89-9 92 28-222

www.simons-voss.com

Digital Locking System 3060

State of: June 2006

Simons Voss technologies

Digital Locking System 3060

Register

1.0 General Method of Operation ____ 3

2.0 The Components of the Digital Locking and Organization System 3060 ____ 3

2.1 Software LDB ____ 3

2.2 Programming ____ 4

2.3 Digital Locking Cylinder 3061 ____ 4

2.4 Digital Smart Relay 3063 ____ 4

2.5 Transponder 3064 ____ 4

2.6 Network 3065 ____ 5

2.7 Block Lock Function 3066 ____ 5

3.0 Digital Components With Access Logging and Time Zone Control ____ 5

3.1 Access Logging ____ 5

3.2 Time Zone Control ____ 6

1.0 General Method of Operation

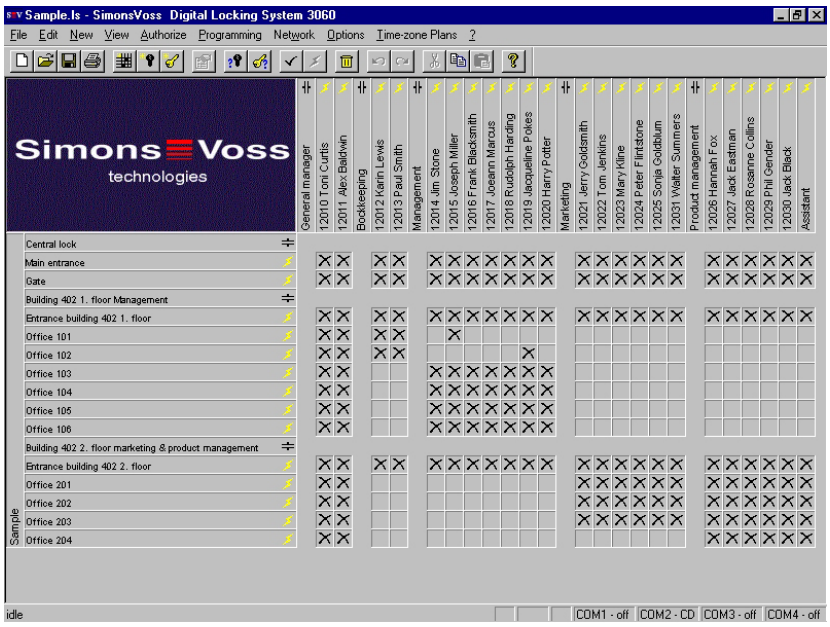
The Digital Locking and Organization System 3060 is modularly constructed and is suitable for uses ranging from a simple locking system for individual doors all the way to a complex PC-controlled access control system. Conventional mechanical keys are replaced by the programmable transponder, which controls doors, gates, barriers, furniture and elevators, for example, over radio transmission. Each transponder is programmed individually for the locking system. The access authorisations are assigned by means of the locking plan. This makes it possible to provide each employee with an individual locking plan with access control and time zone control. The identification in the system and the radio transmission are done by sending and receiving constantly changing crypto codes, thus making the misuse of the system technically practically impossible. Modifications or expansions of the system at a later date are always possible.

2.0 The Components of the Digital Locking and Organization System 3060

2.1 Software LDB

The locking plan software runs under Windows 98, Windows ME, Windows NT/2000 and Windows XP. All components can be programmed as required using the locking plan software. One locking plan can contain a maximum of 16,386 lockings and 8000 transponders. For even larger locking systems, the lockings and transponders are distributed among several locking plans. The locking authorisations are assigned by simply clicking with the mouse. As a result, later modifications are possible with no trouble.

☺ A detailed description is to be found in our Software Operating Instructions!



2.2 Programming

You will need the SmartCD and a PDA for programming the digital components. The data is encoded and then transmitted to the digital components via radio signal.

Another possibility for programming a Digital Locking Cylinder 3061 and Transponder 3064 is with the Programming Transponder 3067. For example, you can issue or change access authorizations in small systems by simply pressing a button when you lose a key or change the locking plan. No PC or special system software is needed.

2.3 Digital Locking Cylinder 3061

The Digital Locking Cylinder 3061 is a compact, powerful access control system that can be installed in any door in only minutes. Its dimensions correspond to those of an ordinary mechanical cylinder that meets the norms. Because the Digital Locking Cylinder 3061 has batteries (master and backup batteries), it can be installed without wires in all Euro Profile doors and can replace already existing
mechanical cylinders. A drop in the battery voltage is indicated by a multilevel warning system (service life approximately 60,000 operations).

2.4 Digital Smart Relay 3063

The SimonsVoss Smart Relay is an electronic switch that can be switched with a SimonsVoss transponder. You can use the SimonsVoss software to configure the authorisation for transponders that are permitted to operate the Smart Relay. In this way, the Smart Relay offers the full function of an access control reader.

2.5 Transponder 3064

The Transponder 3064 is a digital key that can be programmed using SimonsVoss software and that works by radio transmission, without contact. It not only replaces mechanical keys, but also takes over the function of identity cards. Simply pressing a button triggers the encoded communication between the transponder and locking

cylinder, Smart Relay or activation unit.

2.6 Network 3065

The cable-free Network 3065 is an online access control system that administers, visualises and archives all System 3060 information in one central location, and all without manipulations at the door, door frame or the door hardware.
It is especially recommended for medium-sized and large locking systems in order to be able to configure and administer the locking system from a central PC. The LON standard data transmission is done from the PC over the network wiring (twisted pair) and out to the network nodes (LockNodes), which are installed near a digital component. From the LockNode, the data is directed without wires over radio transmission to the digital unit.

☺ While it is true that access to the network software is no longer possible if there is a power failure (unless the network has been protected by a no-break power supply), however, all of the locking system's components that are equipped with a battery still function.

2.7 Block Lock Function 3066

SimonsVoss has the Block Lock Function 3066 in its product line as an option of the Digital Locking and Organization System. This function offers the possibility of activating your alarm system from a central point while at the same time preventing the monitored doors from being accidentally opened during this time. This rules out annoying and expensive false alarms right from the start.

The Block Lock Function 3066 is also available as a VdS version.

3.0 Digital Components With Access Logging and Time Zone Control

3.1 Access Logging

The Plus versions of the digital locking cylinder, SmartRelay and activation unit record the access attempts of authorised transponders. The read-out of the access list from the lockings is done using the SmartCD or, in the case of a networked locking system, over the LockNodes.

A total till 128 accesses (with Smart Relay 1.024), with date, time of day and transponder designation can be stored in the access lists of the separate components. After that, the complete file isn't deleted, but instead the oldest access is always overwritten with the new one.

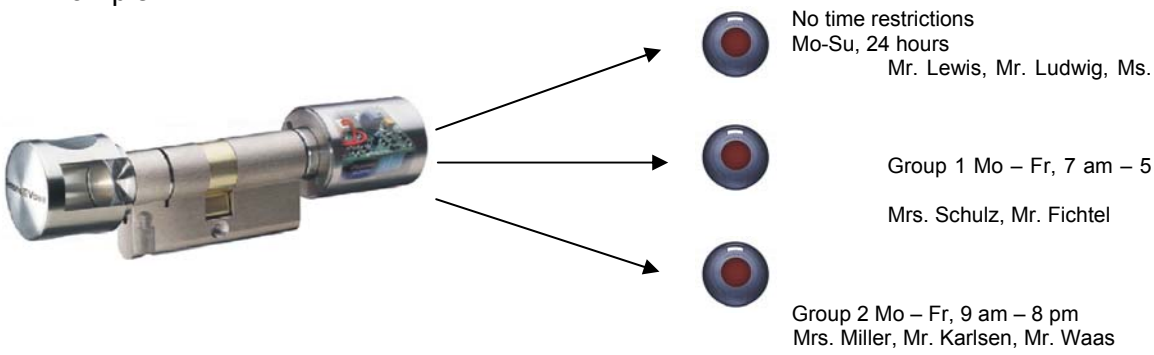
After the access list has been read out with the programming device or network nodes, it is imported into the PC and administered there by the locking plan software. A total of 10,000 accesses can be stored in the PC file. When the data is accepted from the programming device, a comparison is done so that it is always only the current, new accesses that are accepted into the PC file.

3.2 Time Zone Control

You can program lockings in such a way that authorised transponders are authorised for access only at certain times.

Transponders normally have no time restrictions, i.e., that are always authorised for locking 7 days a week, 24 hours a day. However, you can assign transponders to time groups so that they can open or lock at times that can be freely defined. There are five different time groups available (for a more precise description, see the Software Operating Instructions).

Example:


No time restrictions
Mo-Su, 24 hours
Mr. Lewis, Mr. Ludwig, Ms.
Group 1 Mo – Fr, 7 am – 5
Mrs. Schulz, Mr. Fichtel
Group 2 Mo – Fr, 9 am – 8 pm
Mrs. Miller, Mr. Karlsen, Mr. Waas

You can draw up an individual time zone plan for each locking.

☝ It is **not** possible to equip a standard version with the access logging and time zone control functions of the TZC-version at some later time.

Transponder 3064

State of: September 2006

SimonsVoss technologies

Transponder 3064

Content

1.0 Method of Operation 3
1.1 General 3
1.2 Higher Priority Locking Level 4
2.0 Special Models 5
2.1 Password Transponder 5
2.2 Switching Transponder 5
2.3 Explosion Protection Transponder 5
3.0 Explosion Protection Transponder 6
3.1 General Information 6
3.2 Standards 6
3.3 Grouping 6
4.0 Additional Functions 7
4.1 Time Zone Control 7
4.2 Validity Date 7
4.3 Activation Transponder 7
5.0 Battery Replacement 8
5.1 Battery Replacement 3064 8
5.2 Battery Replacement for the Explosion Protection Transponder 8
6.0 Loss of the Transponder 8
6.1 Emergency Opening 8
6.2 Replacement Transponder 8
7.0 Data Sheet 9

1.0 Method of Operation

1.1 General

The Transponder 3064 is a digital “key” that is programmed with the locking plan software and that works over radio transmission with no physical contact. All functions, for example, opening and closing doors, gates, barriers, furniture locks, etc., are carried out by pressing a button. Communication with the digital components (cylinder, Smart Relay and activation unit) takes place by sending and receiving constantly changing crypto codes, which makes misuse practically impossible.

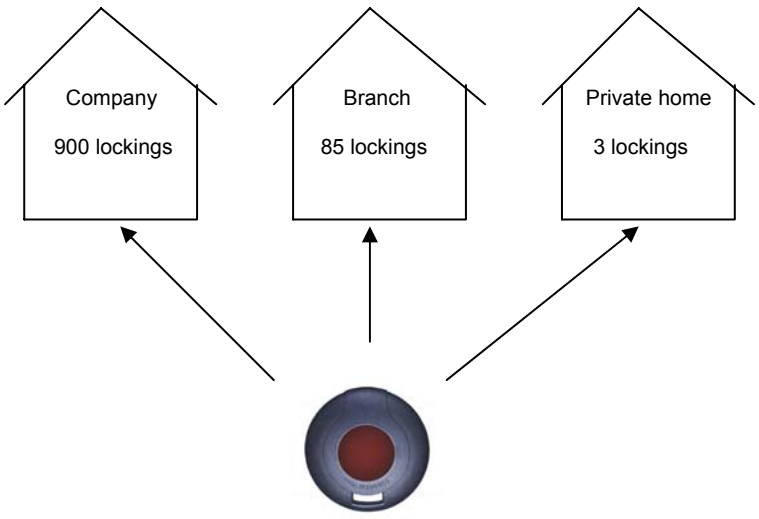
Since the System 3060 works with active transponder technology, the transponder has its own voltage source (battery) available. The advantage in comparison to passive technologies lies in the smaller energy requirements of the cylinder and the larger range.

In order to trigger an action, hold the transponder near the digital locking (refer to the separate chapters for information on maximum transponder ranges) and then press the transponder button. Provided that the transponder is authorised for this digital locking, the desired action, for example, opening or locking the door, can be carried out.

The housing of the transponder is protected against splash water. However it is not waterproof!

Each transponder can be used in three different, mutually independent locking systems (assuming that no validity areas were programmed). Each locking system has its own password and is administered separately.

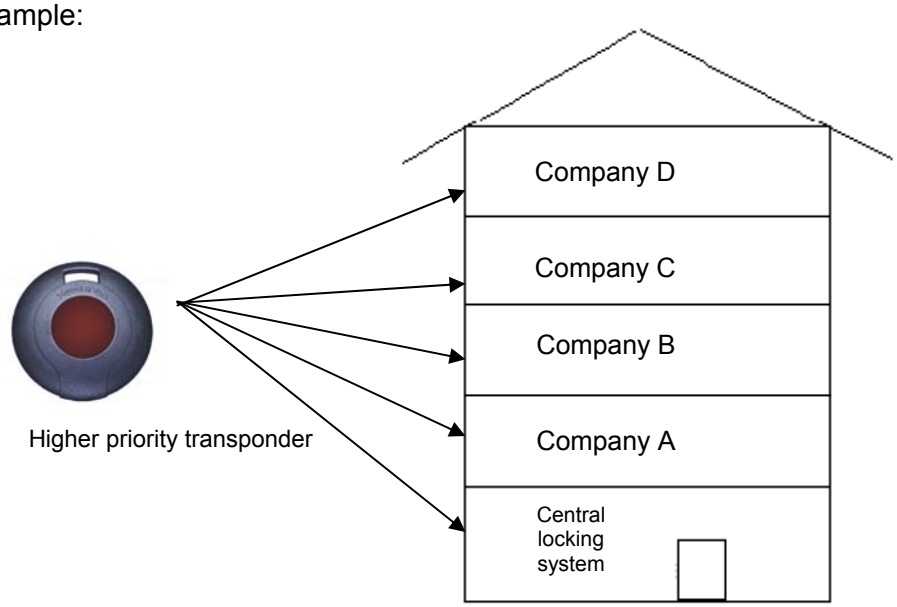
Example:



1.2 Higher Priority Locking Level

If it is necessary to have transponders that are authorised for more than 3 mutually independent locking systems, “higher priority locking levels” must be set up in these locking systems. There are a maximum of 3 higher priority locking levels available for this. All transponders of a higher priority locking level have the same authorisation. One digital locking distinguishes between a maximum of three higher priority levels.

Example:



Four companies are accommodated in an office building with a central locking that is used by all the companies. Each company administers its own locking system with its own password. Every employee receives a transponder that is authorised for 2 locking systems, namely the central locking und his or her own company.

However, the fire brigade, for example, needs a transponder that is authorised for all five of the building’s locking systems. To accomplish this, a higher priority locking level with the same separate password must be set up in all five locking systems and the authorisations must be set up for the higher priority transponders. The transponders set up in this level all have the same authorisation. If higher priority transponders with other authorisations are required, an additional higher priority locking level must be set up (max. 3 higher priority locking levels per locking!). The higher priority transponder must then be programmed into all shutdowns of all 5 locking systems.

2.0 Special Models

2.1 Password Transponder

Instead of manually entering the locking system password, you can transmit it over radio frequency with the help of a special transponder. Standard transponders cannot be used as password transponders.

2.2 Switching Transponder

With this transponder, a two-wire cable (approx. 1m or 37 inches) is connected to the switch contacts of the button and guided outside the device. When both wires are connected, the transponder switches through.

Application examples:

- Connecting external systems
- Remote triggering of a Digital Locking Cylinder or Smart Relay
- Block Lock Function 3066: System activation from more than one location

2.3 Explosion Protection Transponder

This is a transponder with the same functions as the Transponder 3064. In addition, this transponder is released for use in explosion protection zone 1.
(Note Chapter 3 in this regard).

2.4 SmartClip

The special design of this transponder means that the SmartClip is suitable for holding an ISO 7816 format card.

2.5 Transponder, bonded

The standard transponder as described above, but with a glued-shut casing. This prevents end-users from opening the case and using the transponder electronics improperly.

2.6 Transponder, numbered

Sequentially numbered transponders can also be ordered if required.

Explosion Protection Transponder

2.7 General Information

This special product is a transponder that is permitted to be carried into and used in areas subject to explosion hazards, called Zone 1. An area is denoted as Zone 1 when atmospheres capable of exploding occur occasionally. It is crucial that you keep in mind the following issues:

- You are not permitted to open the housing.
- Unlike with the Transponder 3064, only SimonsVoss Technologies AG is permitted to change the battery.
- Normally, you must comply with the general operating instructions of the BGR132 (German rules for occupational safety and health) when using the device in Zone 1.

3.2 Standards

The transponder has been tested according to the applicable explosion protection standards. Refer to:

- Directive 94/9/EC
- DIN EN 50014 (Electrical apparatus for potentially explosive atmospheres)
- DIN EN 50020 (Intrinsic safety "i")

3.3 Grouping

The transponder is grouped in the following way:

- Explosion protection: zone 1
- Intrinsic safety: ib
- Explosion group: IIC
- Temperature class: T3
- Device group: II2 G

This applies to areas in which a potentially explosive atmosphere can arise due to gases, vapours or mists. The information quoted relates to an ambient temperature of from -20°C to +40° C (-4° F to +104° F) in the place of use.

3.0 Additional Functions

The following functions can be activated in the locking plan software:

3.1 Time Zone Control

For TZC version digital lockings, you can program transponders that have locking authorisation for specific times only. These time zones are deposited in the locking plan software, and the transponders are then assigned to an appropriate time zone group.

Example: Mr. Miller receives the following authorisation:

Monday to Friday	from 9:00 am, until 6:30 p.m.
Saturday	from 9:00 am, until 12:45 p.m.
Sunday	no authorisation

3.2 Validity Date

It is possible to program transponders whose authorisation is tied to a validity date (this also applies to non-TZC-versions):

- Transponders that are valid **from a specific point in time** (e.g., from 8:00 a.m. on July 12, 2003
- Transponders that are valid **up to a specific point in time** (e.g., until 5:00 p.m. on July 12, 2003
- Transponders that are valid **for a specific time interval** (e.g., from July 1, 2003 until July 31, 2003)

- One data record is assigned for each activation or expiry date!

3.3 Activation Transponder

Within the scope of the block lock function, all authorised transponders for a digital locking in the security area are blocked when the alarm system has been activated in order to avoid false alarms. For emergency situations, transponders can be programmed (for example, for the fire brigade) that release this block. Afterwards, the door can be opened with an authorised transponder.

4.0 Battery Replacement

4.1 Battery Replacement 3064

If a battery warning occurs, then the transponder battery can be changed at any time (see the Manual on the 3061 Locking Cylinder – Battery warning). Open the casing carefully so that you can see the battery. Open the battery clip and remove the battery, insert a new one, and close the clip. Press the casing back together again.

When you change the battery it is important to ensure that the procedure does not take more than two minutes, that the transponder button is not pressed during that period, and that you do not short the battery – otherwise you may lose data.

Alternatively:

Send the transponder that needs its battery changing to:
SimonsVoss Technologies AG, Eichenweg 6, 07616 Petersberg.

4.2 Battery Replacement for the Explosion Protection Transponder

Attention:
Only SimonsVoss Technologies AG is permitted to change the transponder battery!

5.0 Loss of the Transponder

5.1 Emergency Opening

An emergency opening can be carried out using the SmartCD + PDA (only use devices approved by SimonsVoss) and with the input of the locking system password.

5.2 Replacement Transponder

If a transponder is lost, it can be deleted from the locking plan and a replacement transponder can be set up. When operating the locking system in overlay mode, the lost transponder is automatically blocked as soon as the replacement transponder is activated at the digital locking. (See the Software Operating Instructions Page H3 for programming and procedure information.)

6.0 Data Sheet

Housing	• Made of weather-resistant plastic • Colour: Black • Degree of protection: IP 65 • Diameter: 42 mm • Integrated lithium battery • Max. 1,000,000 operations, or 10 years standby • Access authorisations for up to 48.149 doors • Can be used in 3 mutually independent locking systems

Q3007 Biometric Transponder

State of: September 2006

SimonsVoss technologies

Q3007 Biometric Transponder

Content

1.0 General Instructions ____ 3
1.1 Safety instructions ____ 3
1.2 Product description ____ 3
2.0 Overview of function ____ 4
2.1 Basic information on operation ____ 4
2.2 Operating states ____ 4
2.3 How the transponder works ____ 5
2.4 "Learn" mode: start-up, scanning in fingerprints ____ 5
2.5 Querying the number of fingerprints scanned in ____ 8
2.6 "Recognise" mode: one-off triggering of transponder ____ 9
3.0 "Delete" mode: deleting fingerprints ____ 10
4.0 Transparent mode ____ 10
5.0 Programming the Transponder ____ 11
with the SimonsVoss software ____ 11
6.0 Changing the Batteries ____ 11
7.0 Technical Data ____ 12
8.0 Table of Diode Signals ____ 13

1.0 General Instructions

Please take 15 minutes to familiarise yourself with how your Biometric Transponder Q3007 works with the help of these operating instructions.

1.1 Safety instructions

Caution! – The batteries used in this product could burn or cause a fire if they are not handled properly. Do not charge, open or burn these batteries or heat to over 100°C.
Make sure that the sensor surface is not dirty or scratched. Do not drop the Q3007 or expose it to any other strong impacts.
In addition, please make sure that the initial scanning in of fingerprints is not carried out by unauthorised persons!
We advise you to protect the Q3007 against unauthorised access if possible.
Handling a Q3007 assumes knowledge of how to use SimonsVoss software. Programming should therefore only be carried out by trained specialist staff.
SimonsVoss Technologies AG is not liable for any damage caused by incorrect programming.
An incorrectly programmed or faulty Q3007 can block access via a door. SimonsVoss AG is not liable for the consequences of such an occurrence, such as blocked access to persons who are injured or in danger, material damage or any other damage.

1.2 Product description

The Q3007 differs from normal transponders by the fact that it is also equipped with a highly sensitive Atmel Fingerprint Sensor. In just a few seconds, a high-powered processor in the transponder compares the saved fingerprint with the fingerprint read in by the sensor. In this way, only people whose fingerprints have been scanned in already can use the transponder. This guarantees maximum security against unauthorised use by third parties, e.g. if the transponder is unsupervised, or is lost or stolen. The Q3007 is therefore particularly suitable for applications where a transponder is provided with very many or very specific authorisations, e.g. if one person has a general transponder for all doors or access to high-security areas.

2.0 Overview of function

2.1 Basic information on operation

The Biometric Transponder Q3007 scans fingerprints using a fingerprint sensor. The finger is dragged across the sensor, rather than being pressed against it.

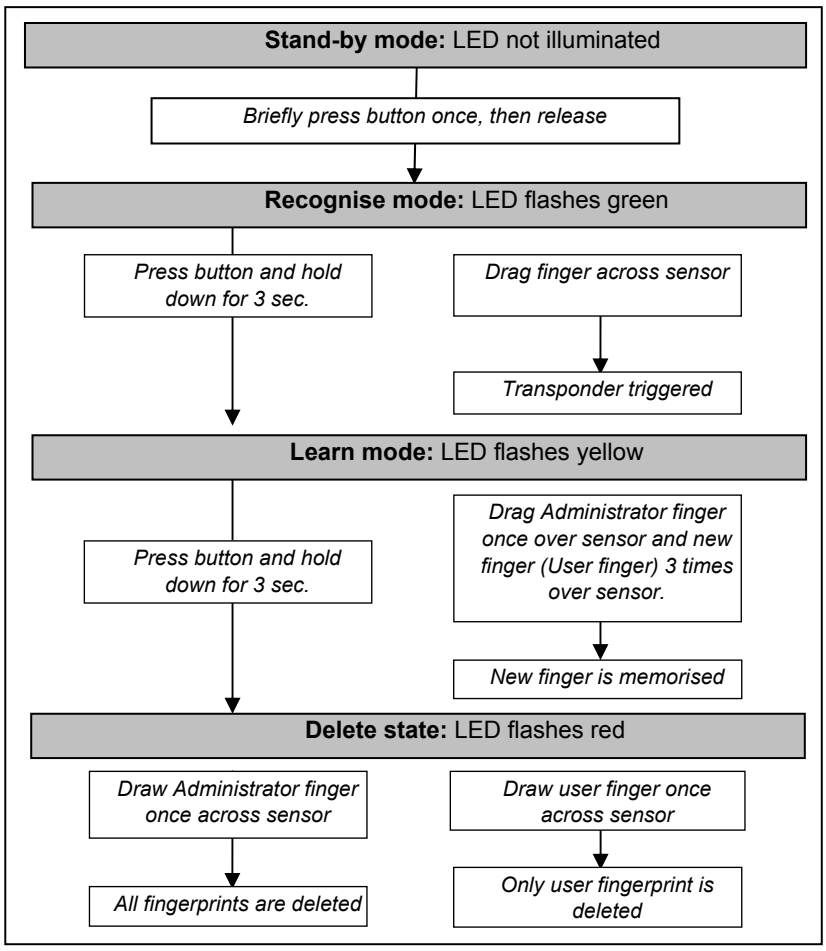
The following should be noted:
The fingerprint to be scanned/ memorised should always be dragged over the sensor in the same way.
To do this, place the tip of the finger that is to be stored or to be recognised at the upper edge of the Biometric Transponder and draw it across the sensor from top to bottom (towards the button) at a constant speed whilst applying slight pressure. The design of the housing means that the finger is guided properly through the slightly raised side walls. This more or less excludes the possibility of using the transponder incorrectly.
The fingerprint sensor can thus pick up the fingerprint line by line and reassemble it into a complete image in the integrated processor. If the reassembled image matches the saved image, the Transponder is released.

2.2 Operating states

The Q3007 has four different operating modes:

Mode	***Function***
Standby	The Q3007 is normally on "Standby" in order to save the battery capacity. After it has completed a function (e.g. scanning), it always returns to the standby mode.
Learn	In the "Learn" mode, new fingerprints can be memorised. Up to 6 different fingerprints can be saved, two of which are what we call "administrator" fingerprints. New fingerprints (user fingerprints) can only be scanned in with the help of an administrator. The only exception is the scanning of the first two fingerprints (Administrator fingerprints), see below
Delete	In the "Delete" mode, fingerprints that have been memorised can be deleted. Individual prints can be deleted, or all fingerprints can be deleted at once.
Recognise	The "Recognise" mode is the mode before a door is opened. In this mode, the Transponder is released if a fingerprint is correctly recognised.

2.3 How the transponder works


Stand-by mode: LED not illuminated
Briefly press button once, then release
Recognise mode: LED flashes green
Press button and hold down for 3 sec.
Drag finger across sensor
Transponder triggered
Learn mode: LED flashes yellow
Press button and hold down for 3 sec.
Drag Administrator finger once over sensor and new finger (User finger) 3 times over sensor.
New finger is memorised
Delete state: LED flashes red
Draw Administrator finger once across sensor
Draw user finger once across sensor
All fingerprints are deleted
Only user fingerprint is deleted

You can interrupt the action in each mode by pressing the button briefly to change to Standby.

2.4 "Learn" state: start-up, scanning in fingerprints

Initial start-up - scanning in the first 2 fingerprints (Administrator fingerprints)
To start the Q3007, two "Administrator fingerprints" need to be scanned in first of all. We recommend that a fingerprint from the left and right hand of one person, the administrator (e.g. safety officer) is used for this. However, you can also use one finger from two different people.

Please note:
The first two fingerprints to be scanned in are automatically (!) the Administrator fingerprints. Without them, no further fingerprints can be scanned in or deleted later!

To scan in and store the first Administrator fingerprint (e.g. left thumb), please do the following:

1. Briefly press the transponder button; the LED will flash green.
2. Then press the button again and hold it pressed for at least 3 seconds (until the LED flashes yellow).
3. Release the button. The system is now ready to scan for 30 seconds, and this is indicated by rapid yellow flashing.
4. **As a high quality of the fingerprint to be teached in is important for good recognition during every day use, please make sure, that your finger to be scanned in is not too dry (e.g. breath on them before having them scanned in)**.
5. Drag finger across the sensor; the LED goes off; after about 1 second, the LED flashes green once to indicate that the fingerprint has been accepted.
6. When the LED flashes yellow rapidly again, drag the finger to be scanned in across the sensor again.
7. Now repeat steps 4 and 5 twice again (so that you have drawn your finger three times across the fingerprint sensor altogether). If an attempt has been unsuccessful (LED is illuminated red), drag your finger across the sensor again.

Using for the first time – 'learning' the first two fingers (Administrator Fingers)

Once the fingerprint has successfully been scanned, the data are saved. This step takes about 2-5 seconds and is indicated by a yellow light flashing at 2 second intervals. The diode is then briefly illuminated green, and the Q3007 returns to Standby.

The Q3007 can now be used by the Administrator, or other fingerprints can be scanned in. Please note that the second fingerprint that is scanned in also has Administrator rights!

Scanning in more fingerprints (User fingerprints)

Further fingerprints (maximum 4) can be scanned in as the Administrator fingerprints have been, except that the Q3007 must first be cleared for this by an Administrator fingerprint. This prevents unauthorised persons from scanning in their own fingerprints and thus gaining access rights that are not allowed.
We recommend that every person who is to use the Q3007 should also be scanned in with two fingerprints, one per hand. This means that three people can be scanned in, with two fingerprints for each one. To scan in more fingerprints, please proceed as follows:

1. Briefly press the transponder button and wait until the LED flashes green.
2. Then press the button again and hold it pressed for at least 3 seconds until the LED flashes yellow, then release the button.
3. Draw the Administrator finger across the sensor; the LED goes off and then flashes green once after about 2 seconds. The system is now ready to scan for 30 seconds, and this is indicated by rapid yellow flashing light. Drag the User finger across the sensor; the LED goes off; after about 1 second, the LED flashes green once to indicate that the fingerprint has been accepted.
4. When the LED flashes yellow rapidly again, draw the finger to be scanned in across the sensor again.
5. Now repeat step 4 twice again (so that you have drawn your finger three times across the fingerprint sensor altogether). If an attempt has been unsuccessful (LED is illuminated red), drag your finger across the sensor again.

Once the fingerprint has successfully been scanned, the data are saved. This step takes about 2-5 seconds and is indicated by a yellow flashing light at 2 second intervals. The diode is then briefly illuminated green, and the Q3007 returns to Standby.
Fingerprints that are already known can always be scanned in, even if 6 fingerprints have already been saved. Unknown fingerprints are then rejected by the LED flashing red twice.

Tips:

- Care in scanning in is rewarded by reliable recognition in use.
- Scanning in the same fingerprint several times improves the quality of the scanned features and thus makes the recognition of the fingerprint more reliable.
- Use a firm base when scanning in fingerprints. We recommend operation with one hand when scanning in thumb prints.
- When scanning in fingerprints, drag the finger across the sensor in a straight line, not too quickly, at an even speed and pressure.
- **Make sure that the sensor is clean and that your fingers are not too dry (e.g. by breathing on them before having them scanned).**

6. Now repeat step 4 twice again (so that you have drawn your finger three times across the fingerprint sensor altogether). If an attempt has been unsuccessful (LED is illuminated red), drag your finger across the sensor again.

Once the fingerprint has successfully been scanned, the data are saved. This step takes about 2-5 seconds and is indicated by a yellow flashing light at 2 second intervals. The diode is then briefly illuminated green, and the Q3007 returns to Standby.
Fingerprints that are already known can always be scanned in, even if 6 fingerprints have already been saved. Unknown fingerprints are then rejected by the LED flashing red twice.

Tips:

- Care in scanning in is rewarded by reliable recognition in use.
- Scanning in the same fingerprint several times improves the quality of the scanned features and thus makes the recognition of the fingerprint more reliable.
- Use a firm base when scanning in fingerprints. We recommend operation with one hand when scanning in thumb prints.
- When scanning in fingerprints, drag the finger across the sensor in a straight line, not too quickly, at an even speed and pressure.
- **Make sure that the sensor is clean and that your fingers are not too dry (e.g. by breathing on them before having them scanned).**

2.5 Querying the number of fingerprints scanned in

You can query the number of fingerprints already scanned in as follows:

1. Press the button once briefly (the LED flashes green)
2. Press the button again and hold it down for 1.5 - 2 seconds (not as long as 3 seconds, which will take you into "learn" mode).
3. The LED flashes red.
4. Then the LED will flash green as many times as the number of fingerprints scanned in (max. 6).
5. The LED flashes red (for a long time if the maximum possible number of fingerprints has been reached, or briefly if it has not).

If no fingerprints have been scanned in, the LED flashes red twice and then returns to Standby mode.

2.6 "Recognise" mode: one-off triggering of transponder

The mode known as the Recognise mode is the normal operating state for the Q3007, i.e. a person whose fingerprint has been scanned in would like to trigger a Transponder signal, e.g. to open a door with a digital locking cylinder or to programme the Transponder within a locking plan.

To do this, proceed as follows:

1. Press the button of the Q3007 briefly (for around 0.5 sec.), and the LED will then flash green.
2. Now drag your scanned finger over the sensor. Make sure that it is in the same position as it was when you scanned it in.
3. If the recognition attempt was successful, the LED shows green and the Transponder is triggered.

If the LED shows red, the recognition attempt was not successful. You can now try three more times. If these are not successful, the Q3007 automatically returns to Standby mode.

Please note:

- It may occasionally happen that the Q3007 does not recognise your finger even though it has been properly scanned in.
- If the fingerprint is rejected with a single red flash, the quality of the fingerprint trace was not adequate. This may be due to the fact, for example, that you did not drag your finger properly across the sensor (too quickly, not straight or not even) or that the surface of the sensor is dirty. If a finger is too dry, it may happen that it "judders" across the sensor. If this happens, please repeat the attempt, or moisten your finger slightly before you do so by breathing on it, for example. With a little practice, however, you'll soon get the knack.
- If the features of your fingerprint cannot be assigned to any of the scanned fingerprints, the diode will flash red twice. You may have accidentally presented a fingerprint that has not been scanned in, or you may have drawn this finger across the sensor quite differently initially from the way you are doing it now (e.g. at an angle, or with more or less of your fingertip in contact with the sensor).

Tip:
Not every fingerprint from a person is recognised equally reliably. If you are often not recognised with one finger, you should perhaps scan in another finger.

Make sure that the sensor is clean and that your fingers are not too dry dry (e.g. by breathing on them before having them scanned)..

3.0 "Delete" mode: deleting fingerprints

Both individually scanned fingerprints and all the fingerprints can be deleted from the memory.

If normal fingerprints (not Administrator fingerprints) are deleted, the other fingers that have been scanned in are not deleted. No Administrator fingerprint is needed to do this (any normal user can delete his own fingerprint).
If one of the two Administrator fingerprints is deleted, all the fingerprints are automatically deleted. The first two fingerprints that are then scanned in are automatically the Administrator fingerprints again.

Fingerprints are deleted as follows:

1. Briefly press the transponder button and wait until the LED flashes green.
2. Then press the button again and hold it pressed for at least 3 seconds until the LED flashes yellow. Release the button.
3. Press the button again and hold it pressed for at least 3 seconds until the LED flashes red. Release the button. You are now in the "Delete" state.
4. Drag finger across sensor.
5. If the first recognition attempt was successful, the LED flashes green. If the fingerprint is a normal one (user fingerprint), only this fingerprint is deleted; if it was one of the two Administrator fingerprints, then all the fingerprints are deleted. Deleting all the fingerprints can take up to 15 seconds. During this time, the diode flashes red every 2 seconds.
6. If the LED flashes yellow, the recognition attempt was not successful. You can now try three more times. If these all fail, the Q3007 automatically returns to Standby mode.

4.0 Transparent mode

It is possible to switch the Biometric Transponder to what is called Transparent mode. In this state, the biometric inquiry is interrupted for 5 minutes and the Biometric Transponder can be used as a normal transponder (doors can be opened simply by pressing a button). At the end of 5 minutes or so, the Biometric Transponder returns to Standby mode.
Transparent mode is required, for example, for setting/cancelling alarms (if an SV Shuntlock VdS is installed) or if several doors need to be passed through in a short time.

To enter Transparent mode, please proceed as follows:

1. Press and hold the transponder button (longer than 1.5 seconds, < 3 sec.). The LED will flash green rapidly. The Transponder will now react to the button as if it were in Recognise mode.
2. Drag finger across sensor (LED shows green if the fingerprint is recognised).
3. The Biometric Transponder is triggered and switches to Transparent mode. The LED flashes red.
4. Pressing the button triggers the system and the LED shows green, followed by red flashing.

After 5 minutes, the Transponder switches off Transparent mode and returns to Standby.
Transparent mode can also be switched off manually by pressing the Transponder button before automatic switch-off until the green LED goes out (approx. 1.5 sec).

5.0 Programming the Transponder with the SimonsVoss software

The "Set validity" function and the "Quasi-proximity mode" are not available for the Q3007.

6.0 Changing the Batteries

To replace the batteries, push the battery cover downwards and remove. Take out all the batteries and replace with new ones. Make sure that the polarity is correct (stamped into the base of the battery compartment).

7.0 Technical Data

Dimensions: H x W x D	65 x 32 x18 mm
Weight	22 g
Colour	Grey, with blue button
Operating distance, locking cylinders	approx. 40 cm (if the transponder (lengthways) is held parallel with the cylinder antenna)
Operating distance, Smart Relay	approx. 120 cm (if the transponder is parallel with the antenna of the Smart Relay)
Protection category	IP 54
Operating temperature range	0°C to 40°C without condensation
Battery type	3 V DC lithium battery type CR-1/3N

8.0 Table of Diode Signals

LED	*Mode*
off	Standby
off	moving finger on sensor followed by comparison with scanned fingerprint, please wait (max. 4 seconds)
Slow green flashing light	Recognise mode, wait for finger (max. 30 seconds)
Fast green flashing light	Release for transparent mode, wait for finger (max. 30 seconds)
One green flash	Successful action (recognise, learn, save, delete, trigger)
Slow yellow flashing light	Release for Learn mode, wait for Administrator finger (max. 30 seconds)
Fast yellow flashing light	Learn mode, wait for finger (max. 30 seconds)
Yellow flashing light	Save scanned finger, please wait (max. 5 seconds)
One or two yellow flashes	Error message in Delete state (cf. 1x or 2x red flashing)
Slow red flashing light	Delete state, wait for finger (max. 30 seconds)
Red flashing light	Delete scanned fingerprint, please wait (max. 15 seconds)
Red flashing light	Transparent state (max. 5 minutes)
Flash red 1x	Action unsuccessful
Flash red 2x	Fingerprint not recognised
Red, 0 to 6 times green, red	Query number of scanned-in fingerprints

BIOMETRIC READER Q3008

State of: August 2007

SimonsVoss technologies

1.0 General information 4
1.1 Safety information 4
1.2 Description of product 5
2.0 Overview of function 6
2.1 Functional overview 6
2.2 Basic operation 6
2.3 Operating statuses 8
2.4 Operation 8
3.0 Programming 9
3.1 Commissioning 9
3.2 Programming additional fingerprints (users) 10
4.0 'Recognize' process 11
5.0 Assigning fingerprints to transponder IDs 12
6.0 Replacing fingerprints 13
7.0 Querying the number of learned fingerprints 14
8.0 Deleting an individual fingerprint 14
9.0 Deleting all fingerprints 15
10.0 Reading the biometric reader 15
11.0 Master finger mode 16
11.1 Commissioning – Programming master fingers 16
11.2 Programming user fingers 17
11.3 'Recognize' process 18
11.4 Deleting individual fingerprints 18
11.5 Deleting all fingerprints 18
11.6 Resetting the biometric reader 19
12.0 Manipulation alarm 19
13.0 Meaning of LED signals 20
14.0 Battery warning 20
15.0 Replacing the battery 21

16.0 Assembly _____ 21
17.0 Special functions _____ 22
17.1 Wireless circuit for SimonsVoss VdS shunt lock 3066_____ 22
17.2 Miscellaneous _____ 22
18.0 Technical data _____ 23

1.0 General information

Please take 15 minutes to read this manual and familiarise yourself with the function of your Q3008 biometric reader.

To assemble the housing you will need a Torx key of size TX6.

1.1 Safety information

Caution! – The battery used in this product may present a risk of fire or burns if misused. Do not charge or open the battery. Do not heat it to over 100°C or burn it. Do not short-circuit.

Only use batteries which have been approved by SimonsVoss.

Dispose of old and used batteries in the correct way. Keep out of the reach of children.

Reversing the polarities may cause damage to the Q3008 biometric reader.

Do not allow the Q3008 biometric reader to become dirty or scratched. Do not drop it or subject it to any other sudden impact.

It is essential to ensure that the device does not come into direct contact with moisture and is not exposed to temperatures below +5°C.

The biometric reader is for indoor use only.

Master finger mode should only be used when the device is installed in a secure indoor location and with a very small number of doors.

Program the reader as soon as it is commissioned to prevent any risk of misuse.

If the reader fails to recognise a finger, or does not recognise it correctly, this does not necessarily mean there is a defect. SimonsVoss Technologies AG accepts no liability for poor recognition caused by skin dryness or the physical structure of the finger.

In order to configure a SimonsVoss biometric reader Q3008 you must be familiar with the product and SimonsVoss software. The Q3008 biometric reader should therefore only be programmed by trained specialists.

SimonsVoss Technologies AG shall assume no liability for damage caused by incorrect programming.

Access through a door may be denied if a Q3008 biometric reader is incorrectly programmed or is defective. SimonsVoss AG shall assume no liability for consequences such as denied access to injured persons or persons at risk, damage to property or any other form of damage.

SimonsVoss Technologies AG reserves the right to make enhancements and modifications to the product without notice. Consequently, descriptions and

representations in this documentation may vary from the most recent product and software versions.

Should there be any variations in the content of other language versions of the documentation, the German original shall apply in the event of any doubt.

This documentation has been produced to the best of our knowledge, but we cannot guarantee that it is free of errors. We therefore offer no guarantee and accept no legal responsibility for the consequences of any errors in this manual.

1.2 Description of product

The Q3008 biometric reader is a digital ‘key’ (transponder), designed to be mounted on a wall, which opens SimonsVoss locks by radio when it recognises an authorised fingerprint. The difference between this reader and, for instance, a PIN code keypad, is that it features a highly sensitive Atmel fingerprint strip sensor. A high-performance processor integrated in the reader compares learned fingerprints with the fingerprints read by the sensor. If the fingerprint is recognised, the reader addresses the lock, which can then be opened. This system offers maximum security against unauthorised use by third parties. This makes the Q3008 biometric reader particularly suitable for applications where only a few doors need to be accessed by just a few members of staff, or for additional security for doors or access to high-security areas.

For the system to be configured, the biometric reader must be programmed with the SimonsVoss programming software and it must learn a finger. Then, when the authorised finger is recognised, the appropriate lock is released.

The Q3008 biometric reader may only be used in indoor areas (IP41). The product has its own power supply and can therefore operate self-sufficiently. Assembly is very simple as there is no need for wiring.

Because of its modular nature, this component can be easily integrated into the SimonsVoss System 3060 and like all SimonsVoss components can be programmed with the locking plan software.

2.0 Overview of function

2.1 Functional overview

The Q3008 biometric reader consists of the following components:

- Biometric analysis unit
- Integrated digital transponder which opens the appropriate lock when triggered by a successful biometric analysis.

The Q3008 biometric reader enables you to address all SimonsVoss locks (e.g. cylinders, smart relays or even arming units, etc.) using biometry.

The reader can learn up to 50 different fingerprints. Each finger is assigned its own transponder ID (TID). In SimonsVoss locks (with time control function, i.e. access control and time zone control) it is also possible to grant an individual time-limited access to a building and to keep a log of who accessed an area and when they did so.

2.2 Basic operation

The Q3008 biometric reader scans fingerprints using a strip sensor. The finger is not placed on the sensor (the small grey rectangle inside the black finger guide) but drawn across it.

Please note:

The learned finger image must be of good quality in order for the reader to recognise your fingerprint quickly and easily later on.

So whether you want the reader to learn or recognise your fingerprint, you must always draw your finger across the sensor in the same way.

Place your finger (the finger to be learned or which has already been learned) in the finger guide, above the sensor. At a constant speed and with gentle pressure, draw your finger down the strip sensor from top to bottom as shown in the pictures (moving towards the LED). Because of the design of the housing, you will find that your finger is guided clearly by the higher side walls. This makes it very difficult to operate the reader wrongly.

The strip sensor reads the fingerprint line by line and reassembles these lines in the integrated processor to form a complete image. If the assembled image corresponds to a stored image, the transponder is triggered.

Figure 1

Activate the biometric reader by placing your finger on the finger guide (see chapter 2.4), and then place your finger at the top of the sensor.

Figure 2

Draw your finger across the sensor at an even speed and applying gentle pressure.

Figure 3

Keep your finger straight and extended, i.e. do not bend or curl it.

When scanning your finger please ensure that your finger remains in contact with the sensor at all times. In other words, you should maintain gentle pressure on the sensor during the scanning process.

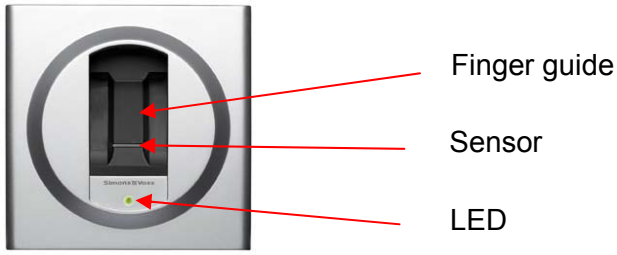
2.3 Operating statuses

The Q3008 biometric reader distinguishes between 5 different operating statuses:

Status:	Explanation:
Standby	The biometric reader is in idle mode and consumes very little power.
Recognize	Recognize mode is the status used before an attempt is made to open a door. Once an authorised fingerprint is recognised, the lock is addressed by radio and can then be opened.
Learn	In this mode, the relevant integrated transponders (up to 50) can be programmed or reset with the SimonsVoss software. The reader can store up to 50 different fingerprints.
Delete	In delete mode, learned fingerprints can be deleted. You can delete individual fingerprints or all fingerprints.
Battery warning	A battery warning system gives you adequate warning when a battery needs replacing.

2.4 Operation

Once the Q3008 biometric reader has been commissioned and configured, it forms a ‘wireless circuit’ with a SimonsVoss lock within the System 3060. The following chapters describe in detail how to program individual fingerprints and the relevant transponder data records and how to use the Q3008 biometric reader.



3.0 Programming

The following chapters describe the programming process in detail. If you are using the biometric reader in a small-scale locking system, please refer to chapter 11.0 Master finger mode.

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery.

3.1 Commissioning

Please note: The 3008 biometric reader must be created in the locking plan as a *lock (biometric reader)* and users as transponder type *biometric reader users*. Users (transponder IDs) and fingerprints can only be learned in situ with the SmartLSM and the SmartCD.

Please proceed as follows:

1. Create a locking plan in the SimonsVoss software.
2. Create 'biometric reader' as a *lock→biometric reader*.
3. Create lock (e.g. locking cylinder).
4. Create transponder using the option *Biometric reader user*.
5. Issue authorisation for the 'biometric reader' and the corresponding lock.
6. Connect the SmartCD to the PC and bring within communication range of the 'biometric reader'.
7. Highlight the biometric reader and launch '**Programming → Lock**' in the programming software. This is where you undertake basic configuration of the biometric reader.
8. Once the reader has been successfully programmed, this is indicated by a pop-up window. This time, the yellow programming lightning symbol remains displayed in the locking plan.
9. Bring the SmartCD into the communication range of the lock to be addressed.
10. Highlight the lock to be addressed by the biometric reader and launch '**Programming → Lock**' in the programming software. This is where you undertake basic configuration of the lock.
11. Once the lock has been successfully programmed, this is indicated by a pop-up window.

    The following programming steps are performed in situ with a PDA and SmartLSM:

12. Export the complete locking plan (pocket PC).
13. Bring the SmartCD into the communication range of the biometric reader.

14. In SmartLSM, launch the '**Read**' locks function. The biometric reader is recognised and read.
15. Select '**Modify transponder**' and start the function by selecting '**Execute**'.
16. Select the appropriate transponder (biometric reader user) and launch the '**Programming**' function.
17. While the transponder is being programmed, the biometric reader automatically switches to Learn mode (LED flashes yellow), and you will be asked to draw your finger over the finger guide.
18. Draw the finger you want the reader to learn over the sensor.
19. If the fingerprint is recognised, the LED on the biometric reader gives two long flashes in green.
20. If programming was successful, the message "Programming successful" appears in the SmartLSM. The fingerprint has been successfully stored.
21. After you re-import the locking plan the programming lightning symbols disappear, both from the transponder and the biometric reader (if all transponders have been programmed).

3.2 Programming additional fingerprints (users)

To learn additional users, proceed as follows:

1. Create transponder using the option *Biometric reader user*.
2. Issue authorisation for the 'biometric reader' and the corresponding lock (e.g. locking cylinder).
3. Fully export the locking plan (pocket PC).
4. Bring the SmartCD into the communication range of the biometric reader in situ.
5. In SmartLSM, launch the '**Read**' locks function.
6. Select '**Modify transponder**' and start the function by selecting '**Execute**'.
7. Select the appropriate transponder (biometric reader user) and launch the '**Programming**' function.
8. While the transponder is being programmed, the biometric reader automatically switches to Learn mode (LED flashes yellow), and you will be asked to draw your finger over the finger guide.
9. Draw your finger over the sensor.
10. If the fingerprint is recognised, the LED on the biometric reader gives two long flashes in green.
11. If programming was successful, the message "Programming successful" appears in the SmartLSM. The fingerprint has been successfully stored in the biometric reader.

12. If you want the reader to learn other fingerprints, repeat from step 4. You must first create additional transponders in the software using the biometric reader user option (see step 1) and assign authorisations to them.
13. Bring the SmartCD into the communication range of the lock to be addressed in situ.
14. In SmartLSM, launch the '**Execute**' function.
15. If programming was successful, the message "Programming successful" appears in the SmartLSM. The new biometric reader users have been successfully stored in the lock.
16. After you import the locking plan the programming lightning symbols disappear, both from the biometric reader user and the biometric reader (if all transponders (biometric reader users) and the corresponding lock have been programmed).

4.0 'Recognize' process

'Recognize' mode is the normal operation for the Q3008 biometric reader, where a person whose fingerprint has been learned wants to open a door using a digital locking cylinder.

Please proceed as follows:

1. When the finger is placed on the finger guide, an integrated proximity sensor activates the biometric reader. After about 0.5 seconds, the LED flashes green.
2. You can now draw your finger (the one learned by the reader) across the sensor, with gentle pressure, making sure that the whole of the top finger joint passes over the sensor (refer to photos in chapter 2.2). Make sure that your finger is in roughly the same position as when the fingerprint was learned.
3. If the fingerprint is recognised and the integrated transponder has been successfully programmed, the LED flashes green twice and the biometric reader is triggered.

If the LED lights up red, fingerprint recognition was not successful. If this happens, you must start again from step 1.
If you moved your finger too quickly over the sensor, the LED gives one rapid flash in red and then turns green again. Draw your finger across the sensor again, this time slightly slower.
If the fingerprint is recognised, the LED will light up green. However, if the lock could not be contacted the LED will light up red again. If this happens, start again from step 1.

Please note:

- The Q3008 may occasionally fail to recognise a fingerprint even though it was correctly learned.

- If a fingerprint is rejected and the LED lights up red, the quality of the scan was not sufficient. This may be because the finger was not moved correctly across the sensor (not straight or not evenly, for example), or because the surface of the sensor is dirty. If the finger is too dry, it may 'judder' across the sensor. Please try again. You may wish to dampen your finger slightly first, for example by breathing on it.
- If the features of your finger could not be assigned to any learned fingerprint, the diode will light up red. You may have inadvertently used the wrong finger. Alternatively, you may have moved your finger differently over the sensor when the reader was learning your fingerprint (for example by turning the finger or with more or less fingertip).

Tip:
A person's fingerprint will not be recognised first time, every time. If you find that a fingerprint is frequently not being recognised, please have the reader learn a different finger.

Dry fingers can make fingerprint recognition more difficult. This can be remedied by moistening your finger or breathing on it, for example.

5.0 Assigning fingerprints to transponder IDs

The maximum of 50 different fingerprints are assigned 50 different transponder IDs. In order to use and differentiate between these 50 different fingerprints, they must be individually programmed.

Each fingerprint is assigned a unique transponder ID (TID). If the locks in a system feature a time control function (i.e. access control), the TIDs are stored in the locks whenever access takes place. This allows you to track which user was given access when.

It is therefore essential to ensure that you keep the same allocations during programming. Otherwise access to the lock may not be guaranteed.

6.0 Replacing fingerprints

You can replace existing fingerprints with new ones at any point, for example if an employee has left the company or no longer requires access through a certain door.

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery.

Please proceed as follows:

1. Open the locking plan with the SimonsVoss software.
2. Export the locking plan (pocket PC).
3. Bring the SmartCD into the communication range of the biometric reader.
4. In SmartLSM, launch the '**Read**' locks function.
5. Select '**Modify transponder**' and start the function by selecting '**Execute**'.
6. Select the appropriate transponder (biometric reader user) and launch the '**Programming**' function.
7. While the transponder is being programmed, the biometric reader automatically switches to Learn mode (LED flashes yellow), and you will be asked to draw your finger over the finger guide.
8. Draw the new finger over the sensor.
9. If the fingerprint is recognised, the LED gives two long flashes in green.
10. If programming was successful, the message "Programming successful" appears in the SmartLSM. The fingerprint has been successfully stored.
11. After you import the locking plan the programming lightning symbols disappear, both from the programmed transponder (biometric reader user) and the biometric reader (if all transponders (biometric reader users) have been programmed).

To replace additional fingerprints, repeat from step 3.

7.0 Querying the number of learned fingerprints

You can query the number of learned fingerprints / transponder IDs at any time. Please proceed as follows:

1. Open the locking plan with the SimonsVoss software.
2. Export the locking plan (pocket PC).
3. Bring the SmartCD into the communication range of the biometric reader.
4. Select the '**Read**' function.
5. Select the '**Modify trans.**' function.
6. Select the '**Execute**' function.
7. You will see a list of all users. Approved biometric reader users are indicated by a thick black cross.

8.0 Deleting an individual fingerprint

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery.

To delete an individual fingerprint, proceed as follows:

1. Open the locking plan with the SimonsVoss software.
2. Remove the cross indicating authorisation from the locking plan by clicking on it.
3. Export the locking plan (pocket PC).
4. Bring the SmartCD into the communication range of the biometric reader.
5. Select the '**Read**' function.
6. Select the '**Modify trans.**' task.
7. Select the '**Execute**' function.
8. Select the relevant transponder.
9. Select the '**Program.**' function.
10. Following successful programming, the SmartLSM will display the message "Programming successful" and a green dot.
11. Re-import the locking plan.

The fingerprint and transponder ID have now been deleted from the biometric reader.

9.0 Deleting all fingerprints

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery.

To delete all stored fingerprints from the Q3008 biometric reader at the same time, you need to completely reset the device. Please proceed as follows:

1. Open the locking plan with the SimonsVoss software.
2. Export the locking plan (pocket PC).
3. Bring the SmartCD into the communication range of the biometric reader.
4. Click on the '**Select**' function.
5. Select 'Biometric reader'.
6. Select the '**Read**' function.
7. Select '**Reset**' and confirm by selecting '**Execute**'.
8. Enter the password for the locking system or take 'From the database' and click on '**Start**'.
9. Re-import the locking plan.

10.0 Reading the biometric reader

It is possible at any time to read the biometric reader and identify programmed transponders using the SimonsVoss locking plan software.

Please proceed as follows:

1. Open the locking plan with the SimonsVoss software.
2. Export the locking plan (pocket PC).
3. Bring the SmartCD into the communication range of the biometric reader.
4. Click on the '**Select**' box.
5. Select the biometric reader.
6. Start the '**Read lock**' function in the SimonsVoss SmartLSM.

11.0 Master finger mode

Master finger mode was developed specially for small locking systems. The biometric reader is programmed once and fingerprints can then be learned simply on the biometric reader itself. No distinctions can be made using different transponder IDs (TIDs), because no TIDs are learned in master finger mode.
Generally, we recommend using SimonsVoss programming software for programming purposes.

You can exit master finger mode at any time. To do this, all learned fingerprints (including the master fingers) must be deleted.

Do not undertake any programming after a battery warning. Replace the battery before proceeding. Refer to chapter 15.0 Replacing the battery**Fehler! Es wurde kein Textmarkenname vergeben.Fehler! Es wurde kein Textmarkenname vergeben.**.

11.1 Commissioning – Programming master fingers

The following chapters describe in detail the programming process for master finger mode.

Please note: The first two fingerprints learned are automatically stored as the master fingers. A master finger cannot also be programmed as a user finger (it will be rejected during the learning process, indicated by 4 red flashes). Unlike normal mode, individual fingerprints cannot be allocated a transponder ID (TID), i.e. the lock does not make a distinction between individual users. In master finger mode it is possible to use the biometric reader to produce an access log for all locks in the same system.

Please proceed as follows:

1. Create a locking plan in the SimonsVoss software.
2. Create ‘biometric reader’ as a *lock→biometric reader*.
3. Create lock (e.g. locking cylinder).
4. Connect the SmartCD to the PC and bring within communication range of the ‘biometric reader’.
5. Highlight the biometric reader and launch ‘**Programming → Lock**’ in the programming software. This is where you undertake basic configuration of the biometric reader.
6. If programming was successful, the programming lightning symbol disappears from the locking plan for the relevant biometric reader.
7. Bring the SmartCD into the communication range of the lock.

8. Highlight the lock to be addressed by the biometric reader and launch '**Programming → Lock**' in the programming software. This is where you undertake basic configuration of the lock.

   Please perform the next steps on the biometric reader itself. The first two fingerprints are automatically stored as the master fingers!

9. Place your finger on the sensor to activate the biometric reader.
10. The biometric reader automatically switches to Learn mode (LED flashes slowly in yellow).
11. Draw the finger to be learned as the master finger across the sensor, for as long as the LED keeps flashing slowly in yellow. (If the LED starts flashing quickly in yellow (indicating time-out), wait until the LED goes out and start again.)
12. If the fingerprint is recognised, the LED gives one long flash in green (fingerprint recognised). The LED gives one more long flash in green. The first master finger has now been stored.
13. To learn the second master finger (which must be different from the first one), please repeat from step 7.

Only once both master fingers have been successfully stored can the reader start learning user fingers. The persons chosen as the master fingers should be the locking system administrator or other persons with direct access to the locking system. As a general principle, ensure that only one finger of each hand is used to program in the master fingers.

11.2 Programming user fingers

Please perform the next steps on the biometric reader itself. The first two fingerprints learned are automatically stored as the master fingers!

1. Place your finger on the sensor to activate the biometric reader. The LED flashes slowly in green.
2. Draw a master finger across the sensor.
3. The biometric reader automatically switches to Learn mode (LED flashes slowly in yellow).
4. Draw the finger to be learned across the sensor, for as long as the LED keeps flashing slowly in yellow. (If the LED starts flashing quickly in yellow (indicating time-out), wait until the LED goes out and start again.)
5. If the fingerprint is recognised, the LED gives one long flash in green (fingerprint recognised). The LED gives one more long flash in green. The user finger has now been stored.
6. To program additional user fingers, repeat from step 1.

11.3 'Recognize' process

Please refer to chapter 4.0 Recognize process.

11.4 Deleting individual fingerprints

To delete an individual fingerprint, proceed as follows:

1. Place your finger on the sensor to activate the biometric reader. The LED flashes slowly in green.
2. Draw a master finger across the sensor.
3. The biometric reader automatically switches to Learn mode (LED flashes slowly in yellow).
4. Wait until the LED flashes quickly in yellow.
5. Touch the finger guide briefly three times with your finger.
6. The biometric reader automatically switches to Delete mode (LED flashes slowly in red).
7. Draw the user finger over the sensor.
8. The LED gives two slow flashes in green. The user finger has been deleted.

11.5 Deleting all fingerprints

To delete all stored fingerprints from the Q3008 biometric reader, you need to delete the complete fingerprint database. Please proceed as follows:

1. Place your finger on the sensor to activate the biometric reader. The LED flashes slowly in green.
2. Draw a master finger across the sensor.
3. The biometric reader automatically switches to Learn mode (LED flashes slowly in yellow).
4. Wait until the LED flashes quickly in yellow.
5. Touch the finger guide briefly three times with your finger.
6. The biometric reader automatically switches to Delete mode (LED flashes slowly in red).
7. Draw a master finger over the sensor.
8. The LED gives two slow flashes in green. All learned fingers (including both master fingers) are deleted.

The biometric reader retains all locking system data. It can now learn new master and user fingers. Once this is done the biometric reader will be available again in the locking system.

11.6 Resetting the biometric reader

To delete all stored fingerprints from the Q3008 biometric reader at the same time (including the locking system data), or if you want to exit master finger mode, you need to delete the complete fingerprint database and reset all locking system data. Please proceed as follows:

1. Open the locking plan with the locking plan software.
2. Select the appropriate biometric reader.
3. Connect the SmartCD to the PC and bring within communication range of the 'biometric reader'.
4. Highlight the biometric reader and launch '**Programming → Reset lock**' in the programming software.
5. Once the lock has been successfully programmed, this is indicated by a pop-up window.

The biometric reader is now back in its original state and can be used for a different locking system.

12.0 Manipulation alarm

After 15 failed attempts, i.e. attempts to operate the biometric reader with a non-programmed fingerprint, the biometric reader reports a manipulation attempt. After each failed recognition, the LED will then flash red for 60 seconds. No fingers will be accepted during this time. Following correct recognition of a fingerprint, the manipulation counter is reset to zero.

13.0 Meaning of LED signals

The LED can light up in three colours: green, yellow and red. These colours have the following meanings:

- Green Reader activated, awaiting fingerprint
  Fingerprint recognised, signal to open sent
  Fingerprint learning process successful

- Yellow Battery warning
  Learn mode

- Red Fingerprint not recognised
  Delete mode
  Fingerprint not recognised during learning process
  Attempt to program master finger as user finger
  Maximum number of learnable fingers reached
  Lock not reached

14.0 Battery warning

The Q3008 biometric reader features a battery warning system to provide information about the status of the device and to minimise operating errors.

The system gives adequate warning of decreasing battery capacity. This alerts you to the need to change the battery in plenty of time.

Battery warning: A time delay is added to the ‘recognise’ process. The diode flashes YELLOW for 10 seconds. Once the 10 seconds have elapsed, the Q3008 biometric reader issues the command to open.

15.0 Replacing the battery

Generally speaking, the battery should only be replaced by a trained specialist. To open the housing you will need a Torx key of size TX6. Please proceed as follows:

1. Fully unscrew the two screws from the base of the housing.
2. Remove the front of the housing.
3. Remove the battery from the holder.
4. Insert the new battery, making sure that the positive terminal is to the right; refer to markings on circuit board. (Please note: polarity MUST be correct!).
5. Reassemble the housing.
6. Screw the two screws back into the base of the housing.

After the battery has been changed, all functions will be available again.

When replacing the battery it is essential to ensure that no water can penetrate into the housing and no electronic parts come into contact with water.

When replacing the battery, and immediately after inserting the battery, be careful not to touch the sensor or finger guide. This could lead to a loss of locking system data.

16.0 Assembly

Generally speaking, assembly should only be performed by a trained specialist. To mount the biometric reader on a wall, near the lock it is intended to open, you can use the screws (including dowels) supplied. To open the housing you will need a Torx key of size TX6. Please proceed as follows:

1. Fully unscrew the two screws from the base of the housing.
2. Remove the front of the housing. Be very careful not to drop the transponder or subject it to any other sudden impact.
3. Drill the appropriate holes in the wall, using the rear panel of the biometric reader as a drilling template if required.
4. Attach the rear panel to the wall using the screws.
5. Reassemble the housing.
6. Screw the two screws back into the base of the housing.

When assembling the unit it is essential to ensure that the sealing ring fits properly, that no water can penetrate into the housing and no electronic parts come into contact with water.

17.0 Special functions

17.1 Wireless circuit for SimonsVoss VdS shunt lock 3066

The biometric reader can be used to activate SimonsVoss arming units (VdS shunt lock 3066). The reader is fitted within the transmission range of the VDS arming unit for this purpose. When the correct fingerprint is recognised, the arming unit is addressed and the alarm system is armed or disarmed via the shunt lock.

For arming/disarming processes, VdS-certified arming units from SimonsVoss require a double opening protocol (double-click if to be armed/disarmed by transponder).

An external software tool from SimonsVoss allows the biometric reader to be reconfigured to shunt lock mode. The configuration emulates the required 'double-click' and the biometric reader is then suitable for arming/disarming processes.

Important: Please only set the double opening protocol (double-click) when using a SimonsVoss VDS shunt lock 3066. Otherwise it could result in malfunction or undesired effects.

You can switch off the shunt lock function at any time using the external tool and return to normal mode.

17.2 Miscellaneous

The quasiproximity, validation and expiry mode functions are not available with the biometric reader.

18.0 Technical data

Dimensions (W x H x D)	96 mm x 96 mm x 21.5 mm
Weight	115 g (incl. batteries)
Material	Plastic
Colour (housing)	Grey
Colour (finger guide)	Black
Number of fingers	50
Number of fingers (master finger programming)	48 users + 2 masters
Maximum number of activations with one set of batteries	Up to 60 000 activations or up to 7 years on stand-by
Operating distance from locking cylinder	Max. 40 cm (if transponder antenna parallel to cylinder antenna)
Operating distance from Smart Relay	Max. 120 cm (Transponder antenna parallel to antenna of Smart Relay)
Protection class	IP 41 (indoor only)
Operating temperature range	+5°C to +50°C
Battery type	1x 3.6 V DC lithium battery, type AA (SL760)
Replacing the battery	To be carried out by trained specialists only
Software	As of LDB 1.52, as of SmartLSM 1.1

PinCode Keypad 3068

State of : September 2006

SimonsVoss technologies

PinCode Keypad 3068

Content

1.0 General information 4

1.1 Safety Remarks 4

1.2 Product Description 5

2.0 Functional Overview 5

2.1 Function Overview 5

2.2 Operating modes 6

2.3 Operating 6

3.0 Start-up 7

4.0 Programming PINs 8

4.1 First Startup 8

4.2 Programming Additional PINs. 8

4.3 Procedure 9

5.0 Deleting PINs 9

5.1 Description 9

5.2 Procedure 10

6.0 Programming the Transponder Data Records with the 10

6.1 Assignment of PINs and Transponders 10

6.2 Description 11

6.3 Procedure 12

7.0 Reading out Transponders 12

7.1 Description 12

7.2 Procedure 12

8.0 Resetting Transponders 13

8.1 Description 13

8.2 Procedure 13

9.0 Opening 14

10.0 Meaning of the LED 14

11.0 Battery Warning 15

12.0 Battery Replacement 15

13.0 Special Functions 17

13.1 Hidden Lock for SimonsVoss VdS Shuntlock 3066 _____ 17

13.2 Miscellaneous _____ 18

14.0 Technical Specification 18

1.0. General information

Please take 15 minutes and read through these Instructions in order to familiarise yourself with the function of your PinCode Keypad..

1.1 Safety Remarks

Caution! Incorrect handling of the batteries used in this product can result in the risk of fire or burns. Do not charge, open or burn these batteries or heat them to more than 100° C (212° F).

Make sure that the PinCode Keypad remains free of dirt and scratches; do not drop the Keypad or otherwise subject it to heavy impacts.

Furthermore, please note that you should program the Keypad with a PIN code immediately after you start it up.

Use of a SimonsVoss PinCode Keypad requires knowledge of the use of the product and of the SimonsVoss software. For this reason, only trained and authorised personnel should program the PinCode Keypad.

SimonsVoss Technologies AG will not accept any liability for damages caused by incorrect programming.
If the PinCode Keypad is incorrectly programmed or is defective, access through a door may be blocked. SimonsVoss AG is not liable for the consequences, such as blocked access to injured or endangered persons, property damage or other damages.
The casing of the PinCode keypad is secured with two Torx screws (TX6) for increased security against unauthorised opening.

1.2 Product Description

The PinCode Keypad 3068 is a digital "key" (transponder), which opens SimonsVoss lockings without contact via radio transmission after the correct numerical codes are entered.

To configure the system, you must first correctly configure at least one PIN and the associated integrated transponder for the locking. The associated locking is then released after a correct PIN has been entered.

The PinCode Keypad that you have purchased is a product that can be used both inside and out. The product has its own power supply, so that it can be operated completely self-sufficiently. Installation is very simple, because absolutely no cabling is required.

Because of the modularity, this component can be seamlessly integrated into the SimonsVoss System 3060, and, like all SimonsVoss components (on the transponder side), it can be programmed with the locking plan software.

2.0 Functional Overview

2.1 Function Overview

The PinCode Keypad comprises the following components:

- PIN code input and evaluation
- Integrated digital key (transponder), which opens the associated locking when it is triggered after the PIN code has been evaluated successfully.

Consequently, the PinCode Keypad allows you to address all SimonsVoss lockings (such as cylinders, Smart Relays, and even activation units, etc.) using the PIN code.

Three different PINs are available, so that individual PINs can be assigned to up to 3 people or groups of people. When a PIN is reprogrammed, only one of up to three user groups needs to be informed. Furthermore, in SimonsVoss lockings (with the time control function, meaning access control and time zone control), it is possible to grant a person or group of people access to a building only during certain times, and to keep a record of which PIN accessed the locking at what time.

2.2 Operating modes

The PinCode Keypad has four distinct operating modes:

Mode:	Explanation:
Standby	The PIN Code Keypad is in standby mode, and uses only very little power.
Opening	After a correct PIN has been entered, the locking is addressed via radio transmission and can be operated.
Programming	In this mode, the following can be programmed or reset: • the individual PINs (max. 3) - directly via the Keypad • or the associated integrated transponders (max. 3) - using the SimonsVoss software
Battery warning	A two-level battery warning system provides plenty of advance notice when it is almost time to change the batteries.

2.3 Operating

After starting up and configuring the PinCode Keypad, it and a SimonsVoss locking represent a so-called "hidden lock" within the System 3060. You can program the PIN directly by making entries on the Keypad. On the other hand, the integrated transponders are programmed by means of the SimonsVoss software, and incorporated into the locking system in this way. The following sections describe the precise procedure for programming individual PIN codes and for programming the associated transponder data records, and the use of the PinCode Keypad.

3.0 Start-up

The first time the system is started up, you will need to replace the factory-set

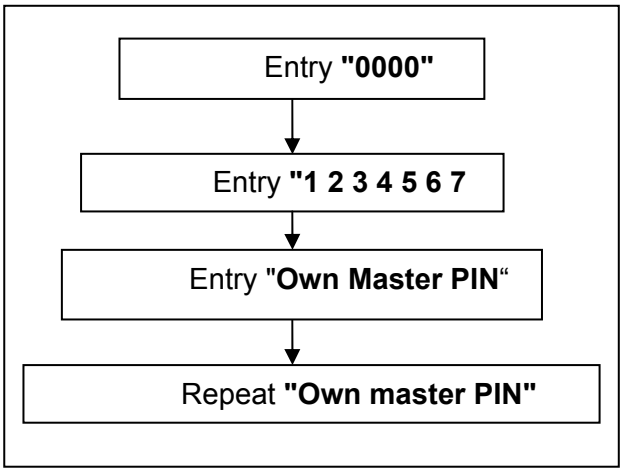
master PIN: **1 2 3 4 5 6 7 8**

with your own master PIN.

Requirement:

- 8 digits
- may not start with a "0"

Your personal master PIN is needed for all programming processes for authentication purposes. Please keep it in a safe place where it cannot be accessed by unauthorised persons.



4.0 Programming PINs

The Master PIN required for all programming procedures is defined by the user (e.g. the System Administrator). Please keep it safe and inaccessible to unauthorised persons, since the Master PIN is required for all programming procedures.

4.1 First Start-up

For the first start-up, the safety of your locking system requires that you program at least one PIN. Only after the PinCode Keypad has been programmed can it be guaranteed that only authorised users receive access.
Proceed as follows:

1. Press the "**0**" to change to programming mode.
2. Enter the "**master PIN** ".
3. Select the PIN that you want to program; in this case, press **"1"** for **"PIN 1".**
4. Enter the length of the PIN (you can choose a number with from **4-8** digits).
5. Enter the "**PIN**"
6. If the input was correct, the PIN is saved and confirmed.

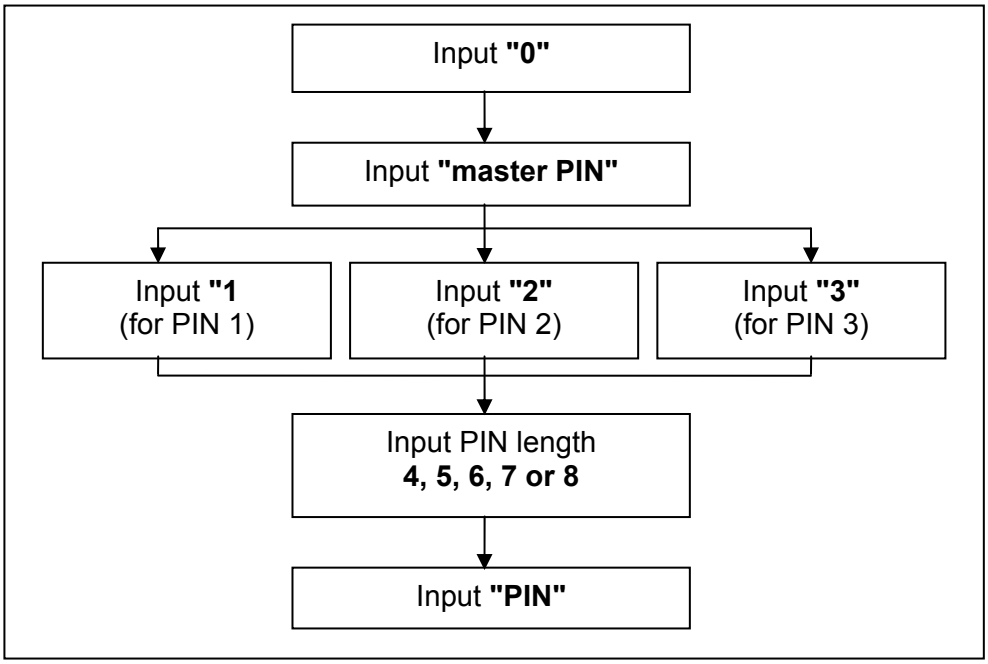
A PIN is not permitted to begin with **"0"** and you may not assign the same PIN more than once. The master PIN is used only for programming the PIN. It is not possible to operate lockings with the master PIN.

4.2 Programming Additional PINs.

1. To program additional PINs, please proceed as follows: Press the "**0**" to change to programming mode.
2. Enter the "**master PIN**".
3. Press
   - **"2"** for **"PIN 2"** or
   - **"3"** for **"PIN 3"**.
4. Enter the length of the PIN (you can choose a number with from **4-8** digits).
5. Enter the corresponding "**PIN**".
6. f the input was correct, the PIN is saved and confirmed.

Attention: It is not possible to enter programming mode when there is a battery warning. This means that when the battery is weak, you cannot change or delete a PIN. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement).

4.3 Procedure



5.0 Deleting PINs

5.1 Description

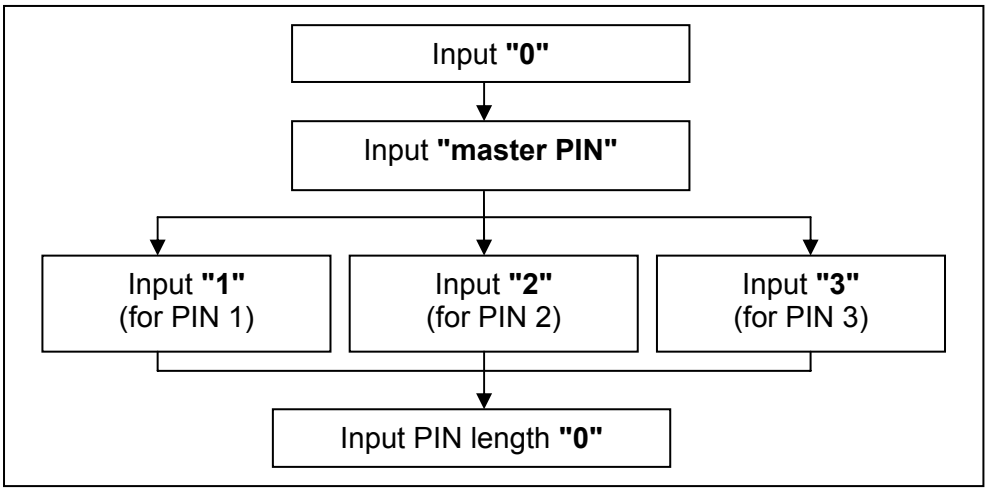
To deactivate PINs again, follow these steps:

1. Press "**0**" to change to programming mode.
2. Enter the "**master PIN** ".
3. Press
   - **"1"** for **"PIN 1"** or
   - **"2"** for **"PIN 2"** or
   - **"3"** for **"PIN 3"**.
4. For the PIN length, enter **"0"**.
5. If the input was correct, the PIN in question is deleted.

In this way, you can deactivate one or more PINs again. They can only be reactivated if you program them again. If you do not need all the PINs, you can leave the extra one unprogrammed.

Attention: It is not possible to enter programming mode when there is a battery warning. This means that it is not possible to change or delete PINs when there is a weak battery. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement).

5.2 Procedure



6.0 Programming the Transponder Data Records with the Simons Voss Software

6.1 Assignment of PINs and Transponders

- PIN1 ⇒ Transponder 1
- PIN2 ⇒ Transponder 2
- PIN3 ⇒ Transponder 3

Each integrated transponder has its own transponder ID (TID); the TIDs are saved in the SimonsVoss lockings when there is an access if the lockings have the time control function (i.e., access control). In this way, you can tell precisely which PIN was granted access and when.

6.2 Description

To program the various transponders with the SimonsVoss software, please follow the procedure described in the following (also see the SimonsVoss "Software Manual"):

1. Press the "**0**" button twice in order to enter the transponder programming mode.
2. Enter the "**master PIN** ".
3. Start the **Transponder programming** function in the SV software
4. For the particular transponder:

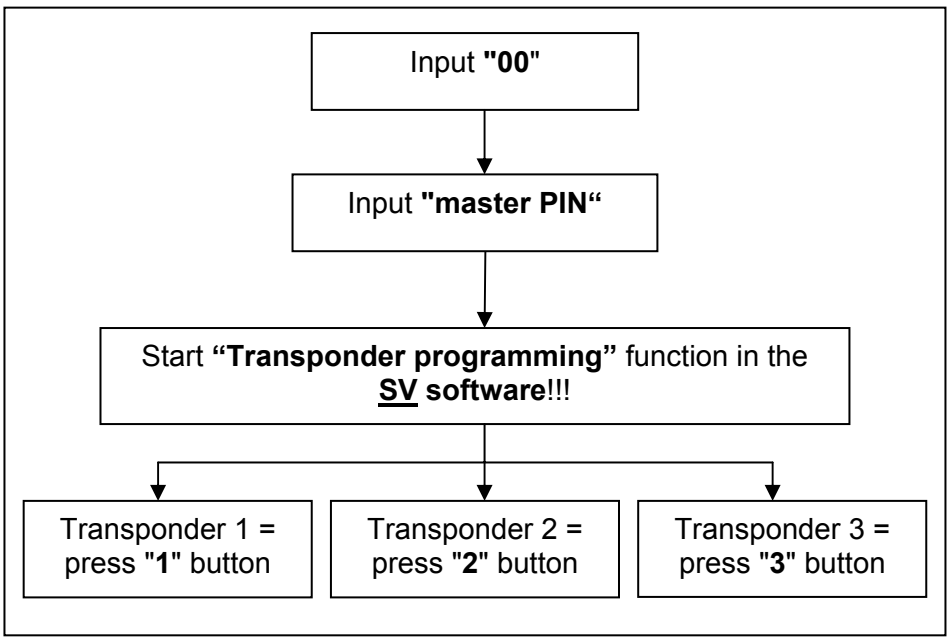
    - Transponder 1 = press the "**1**" button
    - Transponder 2 = press the "**2**" button
    - Transponder 3 = press the "**3**" button

5. Please check in the user interface to see that the programming was successful (yellow programmer flash must have been removed in the locking plan).

In order to be able to carry out the programming without problems, please first start the programming command in the SV software and only then select the required transponder using the PinCode Keypad. Otherwise it is not possible to guarantee successful programming.
The PinCode Keypad's three integrated transponders must be located in the same locking plan as the locking that you wish to address.

Attention: It is not possible to enter programming mode when there is a battery warning. This means that it is not possible to change or delete transponders when there is a weak battery. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement).

6.3 Procedure


Input **"00"**
Input **"master PIN“**
Start **“Transponder programming”** function in the **SV software**!!!
Transponder 1 = press "**1**" button
Transponder 2 = press "**2**" button
Transponder 3 = press "**3**" button

7.0 Reading out Transponders

Anytime it is possible to read out the integrated transponders (after they were programmed) with the SimonsVoss locking plan software.

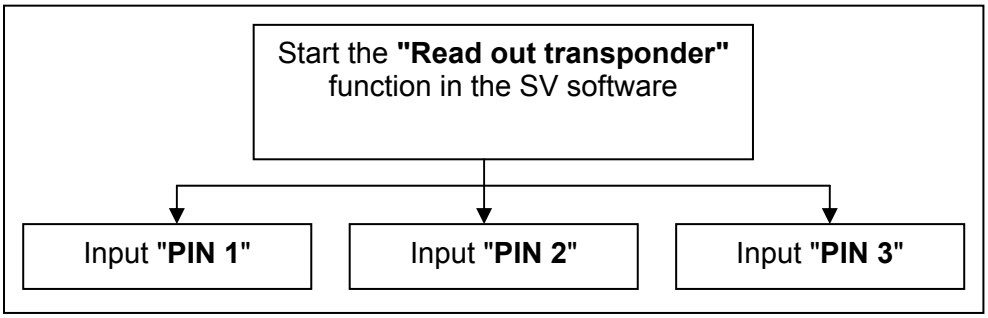
7.1 Description

To do this, proceed as follows:

1. Start the **"Read out transponder"** function in the SV software
2. For the particular transponder:

   - Transponder **1** = enter **"PIN 1"**
   - Transponder **2** = enter **"PIN 2"**
   - Transponder **3** = enter **"PIN 3"**

7.2 Procedure



8.0 Resetting Transponders

8.1 Description

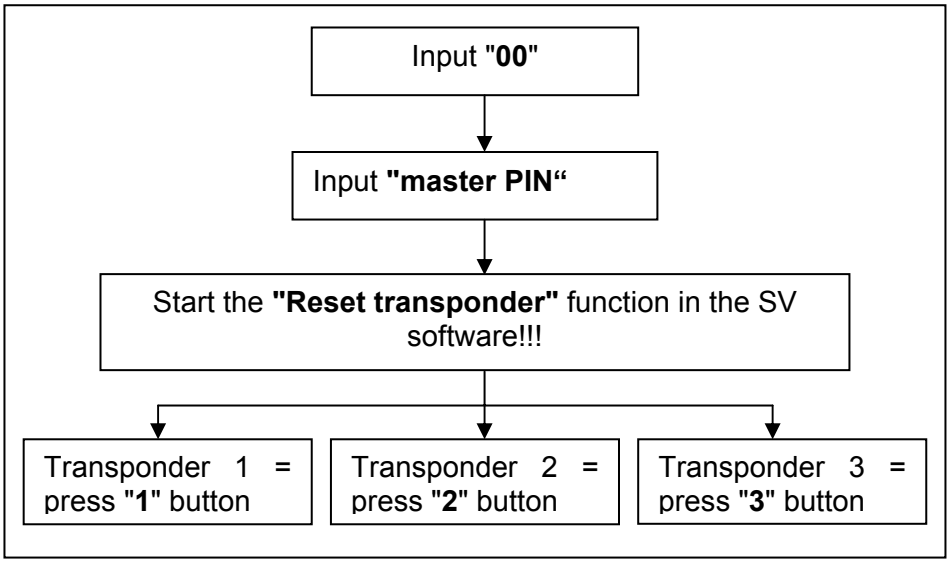
To reset the various transponders, please proceed as follows:

1. Press the "**0**" button twice.
2. Enter the master PIN.
3. Start the "**Reset transponder"** function n the SimonsVoss software.
4. For the particular transponder :

   - Transponder 1 = press "**1**" button,
   - Transponder 2 = press "**2**" button
   - Transponder 3 = press "**3**" button

Attention: It is not possible to enter programming mode when there is a battery warning. This means that when the battery is weak, you cannot reset a transponder. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement).

8.2 Procedure


Input "00"
Input "master PIN"
Start the "Reset transponder" function in the SV software!!!
Transponder 1 = press "1" button
Transponder 2 = press "2" button
Transponder 3 = press "3" button

9.0 Opening

In order to use the PinCode Keypad to open the associated locking, proceed as follows:
Enter a PIN that has already been programmed. You are not permitted to wait more than 5 seconds between the entries of the individual numbers.
In you have entered the correct number and the integrated transponder has been programmed, the LED lights GREEN and a signal is sounded. Then the integrated transponder opens the locking.

10.0 Meaning of the LED

The built-in LED can light in one of three colours: green, yellow and red. These colours have the following meanings:

- Green — Digit that was input has been accepted

  PIN input was OK, which means that
  the correct PIN has been recognised, open signal is being sent

  PIN length OK
  PIN programming procedure was successful

- Yellow — battery warning

- Red — PIN input was incorrect

  Input of master code was incorrect
  Repeated incorrect input of the PIN (manipulation)
  PIN length was not entered correctly.

11.0 Battery Warning

To obtain a defined status for the PinCode Keypad and to minimise operating errors, a 2-level battery warning system has been integrated.

When the battery capacity begins to drop, you will be notified of this in plenty of time to allow you to replace the batteries.

Battery warning level 1: The opening procedure is carried out after a delay. The diode blinks YELLOW and the buzzer sounds for 10 seconds. The PinCode Keypad does not send the open command until after these 10 seconds.

Battery warning level 2: In this case, the opening procedure is again carried out after a delay. The diode blinks YELLOW and the buzzer now sounds for 20 seconds. The PinCode Keypad does not send the open command until after these 20 seconds.

You should not wait any longer to replace the battery. Otherwise, the system will stop functioning after a short time.

12.0 Battery Replacement

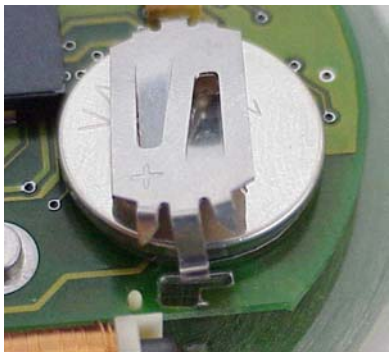
In general, the batteries must be replaced by trained experts only. To do this, proceed as follows:

1. Completely unscrew the two screws in the bottom of the housing.
2. Remove the front of the housing.
3. Carefully release the battery clip from the printed circuit board (Figure 1).
4. Remove both batteries (Figure 1).
5. Insert the new batteries; the positive pole must be pointing up (Figure 2).
6. Carefully hook the battery clip back into the printed circuit board (Figure 3).
7. Put the housing back on.
8. Screw the two housing screws back into the housing from below.

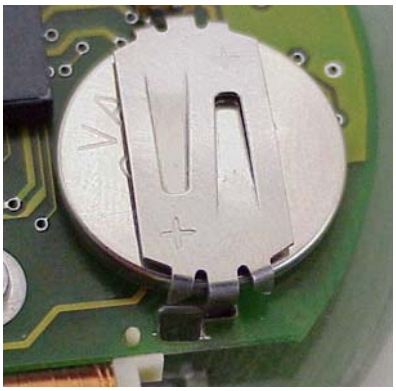
After you have replaced the batteries, all functions will be available again.
Please always replace both batteries at the same time, because they have been charged to approximately the same level.

When replacing the batteries, be absolutely sure that no water is allowed to penetrate into the housing and that the electronics do not come into contact with water. If necessary, carefully wipe dry the housing section that is attached to the wall.

(picture 1)



(picture 2)



(picture 3)

13.0 Special Functions

13.1 Hidden Lock for SimonsVoss VdS Shuntlock 3066

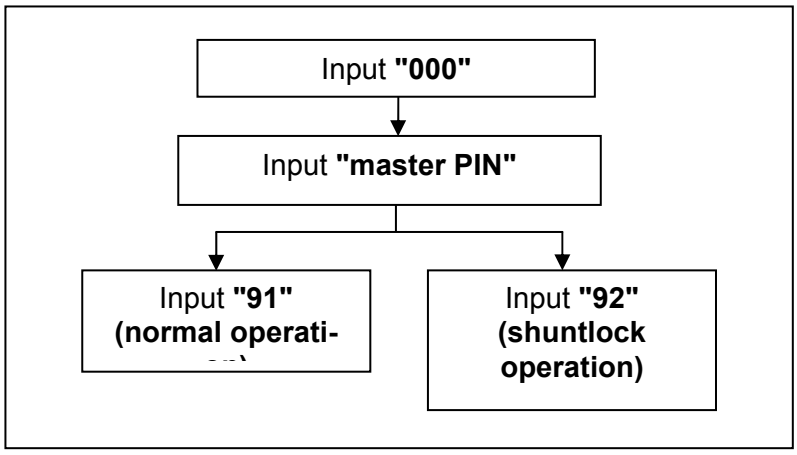
The PinCode Keypad can be used for activating SimonsVoss activation units (VdS Shuntlock 3066). This is done by mounting the Keypad within the transmitting range of the activation unit. After you have input the correct PIN, the activation unit is addressed and the alarm system is activated or deactivated via the shuntlock. This allows the requirements of VdS Class C up to SG 6 to be fulfilled by including a hidden lock.

The VdS-certified activation units from SimonsVoss need a doubled opening protocol for activation/deactivation procedures (double-click when the transponder should activate or deactivate the system).

The following explains the configuration of the PinCode Keypad in order to have it emulate the "double-click" and consequently be suitable for carrying out activation/deactivation procedures. To set the configuration for this purpose, proceed as follows:

1. Press the "**0**" button three times.
2. Input the master PIN.
3. Then press:

   - either **"91"** for normal operation (default setting)
   - or **"92"** for a double-click for shuntlock operation.



If the input was correct, the PinCode Keypad stores the change and gives a positive acknowledgement (LED and buzzer).

Important: Please set the two-time opening protocol (double-click) only when you are using a SimonsVoss VdS Shuntlock 3066. Otherwise, there may be malfunctions or unwanted effects.

You can switch from one configuration to the other at any time.

Attention: It is not possible to enter programming mode when there is a battery warning. This means that when the battery is weak, you cannot change or delete any functions. Programming mode will only be available again after you have successfully changed the battery (see the section "Battery Replacement).

13.2 Miscellaneous

The quasi-proximity and validity and expiry mode functions are not available with the PIN Code Keypad.

14.0 Technical Specification

Dimensions W x H x D	96 mm x 96 mm x 14 mm
Weight	102 g (incl. batteries)
Material	Plastic
Colour	Grey with transparent ring
Maximum number of operations with one battery set	Approx. 100,000 operations or 10 years on standby
Operating distance from locking cylinder	Up to a max. of 40 cm (when the transponder antenna is parallel to the cylinder antenna)
Operating distance from SmartRelay	Up to a max. of 120 cm (when the transponder antenna is parallel to the SmartRelay antenna)
Protection class	IP 65
Working temperature range	-20° C to 50° C (-4° F to 50° F) without moisture condensation
Battery type	2 x 3 V DC lithium battery type CR2032
Battery replacement	Only by trained personnel

Digital Locking Cylinder 3061 VdS

State of: September 2006

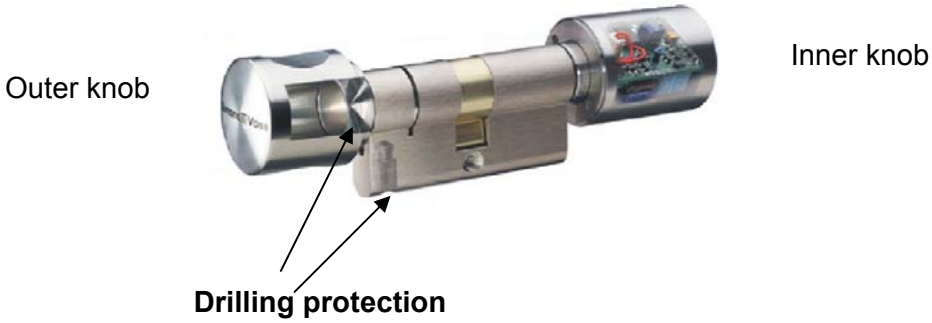
SimonsVoss technologies

1.0 Method of Operation 3
1.1 General Information 3
1.2 Opening and Locking From Outside 3
1.3 Opening and Locking From Inside 3
2.0 Special Models 4
2.1 FH Version 4
2.2 Overview 4
3.0 Additional Functions 4
3.1 OMRON 4
3.2 Extending the Coupling Time 4
3.3 Logging Unauthorized Access Attempts 5
3.4 No Acoustic Programmer Acknowledge 5
4.0 Battery Warnings 5
4.1 Locking Cylinder 5
4.2 Transponder 6
5.0 Battery Replacement 6
6.0 Installation Instructions 7
6.1 General Information 7
6.2 Programming the Locking Cylinder 7
6.3 Removing the Outer Knob 7
6.4 Inserting the Digital Cylinder Into the Lock 8
6.5 Screw On the Outer Knob 8
6.6 Perform Function Test 8
7.0 Potential Applications 8
7.1 General Information 8
7.2 Fire Protection Doors 8
7.3 SLP Locks 8
8.0 Data Sheet 9

1.0 Method of Operation

1.1 General Information

The Digital Locking Cylinder 3061 VdS meets the requirements of VdS (Association of German Property Insurers) Class B and its outer dimensions exactly match those of a standard mechanical cylinder. In comparison to mechanical systems, it excels because it is very easy to install, provides greater security, is more flexible and costs less to operate. It can quickly and easily replace existing mechanical cylinders in "old systems".



1.2 Opening and Locking From Outside

When not activated, the outer knob turns freely. It is not possible to open the door or to lock it. Hold the transponder at a distance of approximately 10 to 40 cm (4 to 16 inches) from the digital locking cylinder and briefly press the transponder button once. If this is an authorised transponder, a double signal tone sounds and the cylinder couples. Now turn the outer knob in the locking or opening direction. You have approximately five seconds for this process. You can use the software to adjust the coupling time. The longer the coupling time, however, the shorter the service life of the battery. Then a single signal tone sounds and the outer knob turns freely again. Make sure that the outer knob of the locking cylinder turns freely again after the coupling process.

- If this transponder is not authorised at this time because of the time zone plan, a single signal tone sounds. The cylinder does not couple, however, and you cannot open the door.

1.3 Opening and Locking From Inside

It is always possible to open doors with Digital Locking Cylinder 3061 VdS devices from the inside without operating the transponder

2.0 Special Models

The standard Digital Locking Cylinder 3061 VdS is equipped as a TZC version, which means that the following functions are always included:

Access logging	The locking cylinder stores the last 128 accesses with date, time and the user name of the transponder. You can read out the data with the PalmCD2 or over the network.
Time zone control	You can program locking cylinders in such a way that authorised transponders are authorised for access only at certain times.

The Digital Locking Cylinder 3061 VdS is also available in the following optional versions:

2.1 FH Version

For doors with thick metal inserts (such as fire protection doors) or with a large screening effect. This version is also used in areas with strong interference fields, such as in server rooms.

2.2 Overview

Locking Cylinder (TZC)
- Entrance doors
- Residential doors
- Office doors
- Interconnecting doors

Locking Cylinder FH (TZC)
- Fire protection doors
- Aluminium doors

3.0 Additional Functions

You can activate the following functions with the software settings:

3.1 OMRON

All product versions can be operated in OMRON mode. You will find a detailed description in the Smart Relay manual.

3.2 Extending the Coupling Time

The default time for the coupling of the cylinder is approximately 5 seconds. You can use the software to extend this time to approximately 10 seconds. This shortens the lifetime of the battery, however.

3.3 Logging Unauthorised Access Attempts

For cylinder version 10.2 and later and in combination with the LDG Version 1.40, it is possible to log unauthorised access attempts, as well as authorised accesses. This includes both access attempts without authorisation and access attempts outside the specified time zone. In this connection, however, only transponders from the locking system are logged, which means that the transponder must have the same locking system ID (SID).

3.4 No Acoustic Programmer Acknowledge

When programming over the network, it can be advantageous to deactivate the acoustic programmer acknowledge. You can do that with this function.

4.0 Battery Warnings

4.1 Locking Cylinder

Warning level 1 for main battery
If the main battery of the locking cylinder goes empty, eight short signal tones, coming quickly one after another, sound after you operate the transponder and before the cylinder couples. You must replace both batteries now.

Warning level 2 for backup battery (SW Version 10.0 & SW Version 10.1)
In addition to the main battery warning, an additional eight short signal tones, coming quickly one after another, now sound for the backup battery warning. The cylinder does not couple until after the signals. From now on, the backup battery is active. You must replace both batteries as soon as possible.

Warning level 2 for backup battery (SW Version 10.2 and later)
Now the signal tones of the backup battery warning sound for only approximately 30 seconds (without the main battery warning). The cylinder does not couple until after the signals. From now on, the backup battery is active. You must replace both batteries as soon as possible.

Warning level 3 (SW Version 10.2 and later)
If you continue to ignore this backup battery warning, either the door can be used 50 more times or the cylinder switches off after 4-5 weeks if there is no further operation. In both cases, the cylinder switches into the so-called storage mode. After this, you can only open the cylinder with the programming device.

4.2 Transponder

If the transponder battery voltage is coming to an end, eight short signal tones, coming quickly one after another, sound each time the transponder is operated on the locking cylinder after the uncoupling.

- Attention: Do not take out the transponder battery because this will probably result in the loss of data. See the “Transponder 3064” manual for more information.

5.0 Battery Replacement

Only authorised personnel are permitted to replace the battery. Use only batteries that are supplied by SimonsVoss.

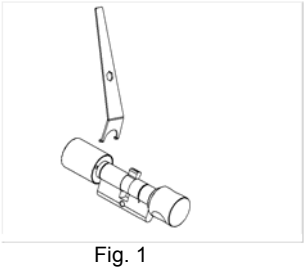


Fig. 1

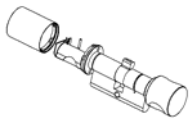


Fig.2

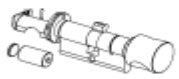


Fig.3

Use the special tool to loosen the locknut (Fig. 1) on the inner knob (long knob) approximately one rotation (only loosen slightly, do not unscrew completely). Carefully push the inner knob back and forth so that the sealing cone loosens and then unscrew the inner knob completely (Fig. 2).

Note: Only push the inner knob to the side very lightly because otherwise you may damage the electronics.

- When changing batteries, always change both batteries.

Insert the main battery into the holding device with the positive pole toward the door and the backup battery in the opposite direction (Fig. 3).

- Reversing the polarity can result in damage to the locking cylinder. Incorrect handling of the batteries used in this device can result in the risk of fire or burns. Do not charge, open, heat to more than 100 C (212 C) or burn. Replace the batteries only with original batteries supplied by SimonsVoss.
- Please dispose of lithium batteries immediately when discharged. Store away from children, do not open and do not throw into fire.
- Never operate the cylinder without a main battery because otherwise the entire power consumption of the cylinder runs over the backup battery.

Fix the lock nut in position with the special tool and press it against the flange. Now turn the inner knob onto the screw thread until the stop and tighten the locknut firmly. Now operate an authorised transponder and test the function.

- Please dispose of discharged lithium batteries immediately. Store away from children, do not open and do not throw into fire.

- You must reset the time of day after the battery change because the clock does not work without current (Software Operating Instructions: Programming → Setting the Clock on the Locking).

6.0 Installation Instructions

6.1 General Information

When installing the Digital Locking Cylinder, make sure that there are no sources of interference in the vicinity. You should install locking cylinders at least 0.5 m (approximately 1.5 feet) from one another and control units or Smart Relays at a distance of at least 1.5 m (approximately 5 feet). The PC housing of the half cylinder is not allowed to stick out into the exterior area more than 3 mm. If necessary, attach a profile cylinder rosette. Furthermore, you must ensure that no water can penetrate the cylinder in the area of the catch

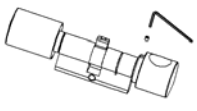
6.2 Programming the Locking Cylinder

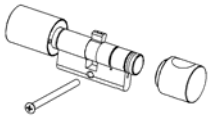
You must program the Digital Locking Cylinder and accompanying transponders in the locking plan before you install them. Please refer to the Software Operating Instructions for more detailed information.

- The locking cylinders are delivered in so-called storage mode, which means that no communication is possible with the transponder (exception: programming transponder). You can also use software and the programming device to remove the storage mode. Please refer to the Software Operating Instructions for more detailed information.

6.3 Removing the Outer Knob

Loosen the setscrew on the outer knob (short knob) with a 1.5 mm Allan key (do not screw the whole way off). Operate an authorised transponder and hold the inner knob still. The locking cylinder couples and you can unscrew the outer knob by turning it counterclockwise.





6.4 Inserting the Digital Cylinder Into the Lock

First turn the lock pin until it is pointing straight down. Then insert the Digital Locking Cylinder through the lock so that the inner knob (long knob) points toward the inside of the door. Fasten the cylinder with the lock screw included in the delivery

Never hit against the knobs during installation. Do not bring the cylinder into contact with oil, paint or acid.

6.5 Screw On the Outer Knob

Screw the outer knob on the screw thread, fixing it in position with your fingers if necessary. Then operate the transponder. Hold the inner knob still and tighten the outer knob solidly. Finally, tightly screw the setscrew with the Allan key.

6.6 Perform Function Test

1. With the door open, turn the inner knob in the locking and opening directions. The knob must turn easily.
2. Close the door and repeat the process. If the locking cylinder is stiff, you must align the door or correct the edge plate.
3. Then perform the same test on the outer knob. To do this, operate an authorised transponder near the cylinder.

7.0 Potential Applications

7.1 General Information

The Digital Locking Cylinder fits locks for Euro Profile Cylinders that meet DIN 18254 specifications.

7.2 Fire Protection Doors

It is possible to install the locking cylinder in fire protection doors. In this case, use the Locking Cylinder Version FH. The approval for a fire protection door is always unaffected by the locking cylinder.

7.3 SLP Locks

The Digital Locking Cylinder 3061 FD is used for applications of this type. The Digital Locking Cylinder 3061 VdS does not have approval for SLP doors at this time. See the “Digital Locking Cylinder 3061” manual → “Possible Applications.

8.0 Data Sheet

Knobs	Material	Stainless steel
	Colours	Brushed stainless steel Brass
	Diameter	30 mm
FH cylinder knobs	Material	Outer knob stainless steel, inner knob plastic
	Colour	Black
	Diameter	30 mm
Profile cylinders	Standard length	Outside 30 mm, inside 30 mm
	Construction length	In 5 mm increments (no kit) up to a total length of 140 mm, where one side of the cylinder can have a max. length of 90 mm. Other lengths upon request.
Battery	Type	Lithium 3.6 V, 1/2 AA Lithium 3 V, CR1220 Use only original replacement batteries from SimonsVoss
	Service life	Approx. 60,000 operations, or 4 years Standby or approx. 4 years
Environmental Conditions	Operating temperature	-20°C to +50°C (-4° F to +122° F)
	Storage temperature	-35°C to +50°C (-31°F to +122°F)
	Degree of protection	IP54 (when installed)

DIGITAL LOCKING CYLINDER 3061

Status: May 2007

SimonsVoss technologies

1. General 4
1.1 Notes on safety 4
1.2 Product description 5
1.3 Design 5
1.4 Opening and locking from the outside 6
1.5 Opening and locking from the inside 6
2. Versions 6
2.1 Standard version 6
2.2 ZK version 7
2.3 FH version 7
2.4 TS version 7
2.5 MS version 7
2.6 VdS version 8
2.7 AP version 8
2.8 WP version 9
2.9 Overlengths 9
2.10 Overview 10
3. Programming and configuration 11
3.1 Access Control 11
3.2 Time zone control 11
3.3 Overlay mode 12
3.4 Extended activation 12
3.5 OMRON 12
3.6 Warehouse mode 12
3.7 No acoustic confirmation signals 13
3.8 Logging unauthorised access attempts 13
3.9 Time-switch function 13
3.10 Flip-Flop 14
4. Status reports 15
4.1 Battery condition critical 15
4.2 Emergency battery activated 15

4.3 Deactivated 15
4.4 Emergency connection activated 16
4.5 Time-controlled opening active 16
4.6 Engaged 16
5. Installation instructions 16
5.1 General notes 16
5.2 Programming the locking cylinder 17
5.3 Installing twin-knob cylinders (except Type .AP) 18
5.4 Installing the anti-panic cylinder (Type .AP) 20
6. Battery warnings 22
6.1 Locking cylinder 22
6.2 Transponder 24
7. Signal tones 25
8. Battery change 25
8.1 General notes 25
8.2 Procedure 26
9. Possible uses 27
9.1 General 27
9.2 Fire doors 27
9.3 Doors on escape routes 27
9.4 Outdoor installation situations 27
10. Accessories 28
10.1 Knobs 28
10.2 Core protection adapter set 28
10.3 Tools 28
10.4 Battery set 28
11. Data sheet 29

1. General

1.1 Notes on safety

- Lock installation and battery changes should only be carried out by trained personnel.
- The cylinder must not come into contact with oil, paint or acids.
- Only use batteries approved by SimonsVoss (see chapter 11).
- The batteries used in digital locking cylinder 3061 can cause a fire or burns if handled incorrectly. Do not charge, open, heat up or burn batteries. Do not short-circuit.
- Dispose of old or used batteries properly, and keep them out of the reach of children.
- Reversing polarity can result in damage to the locking cylinder.
- Always replace both batteries at the same time.
- When replacing batteries, do not touch the contact areas on new batteries. Always use clean, grease-free gloves.
- Cylinder operation requires two batteries.
- Use the .WP version for outdoors installations.
- The locking cylinder's internal knob (electronic side with keypad) complies with Protection Class IP40. It must therefore be ensured that the knob does not come into contact with water.
- SimonsVoss Technologies AG shall not be liable for damage to doors or components resulting from incorrect installation.
- An incorrectly installed or incorrectly programmed cylinder can block access through a door. SimonsVoss Technologies AG shall not be liable for any consequences of incorrect installation, such as lack of access to injured persons, material damage or other damage.
- Alterations and technical developments reserved.
- This documentation was prepared to the best of our knowledge; however errors cannot be completely ruled out. No liability is accepted in this event.
- The content of the German original shall overrule in case of differences in the content of foreign-language versions.

1.2 Product description

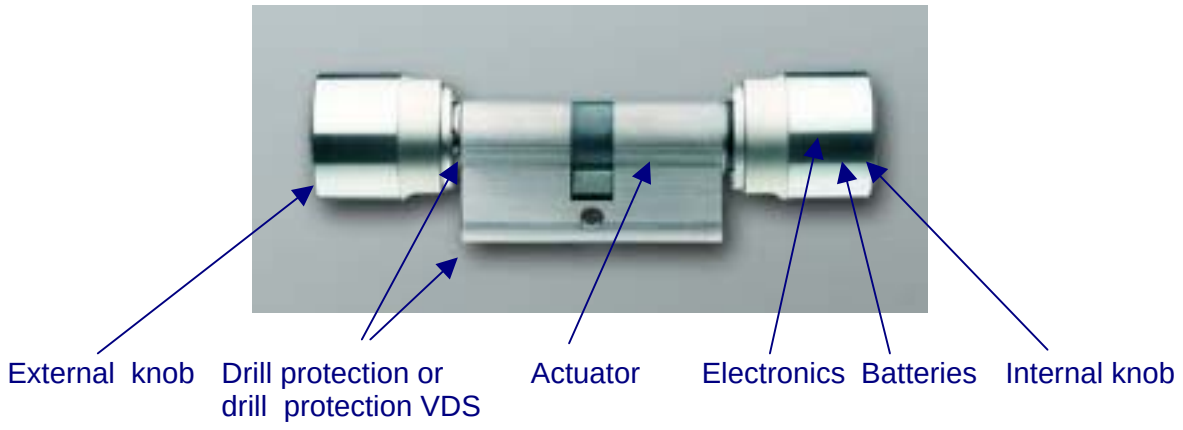
Higher security, greater flexibility, lower cost, network-capability without any wiring in doors and frames, low installation effort - all this is possible right now with the digital locking cylinder 3061. The outer dimensions of the digital locking cylinder are exactly the same as those of DIN 18254 and EN 1303; retrofitting to standard locks is possible at any time. It is quick and easy to exchange.

Adding new functionality to the locking cylinder's scope is made possible by upgradeable firmware. Your investment is thus protected, as "retrofitting" new functions is an uncomplicated matter.

The System 3060 has a modular design that makes it easy to install further cylinders to subsequent extensions and to manage them online as a wireless network. An integrated voltage supply makes cylinder operation self-sufficient and independent from a mains power supply. There is no need for any wiring whatsoever.

All system components are fully integratable with the SimonsVoss System 3060 thanks to system modularity; every SimonsVoss component is programmable using the locking plan software.

1.3 Design



1.4 Opening and locking from the outside

The external and internal knobs rotate freely when deactivated. The door cannot be opened or locked. Hold the transponder approximately 10 to 40 cm from the digital locking cylinder and briefly press the transponder button. If you are using an authorised transponder the locking cylinder will emit a short double signal tone and subsequently engage. Turn the internal or external knob in the direction of opening or locking. You have approximately five seconds for this operation. (The engaging time can be extended to 10 seconds using the software. This will not shorten battery life.) The locking cylinder will emit a single signal tone and the internal or external knob will again rotate freely. Make sure the internal or external knob rotates freely again after the engaging process.

- If you are using a transponder that is momentarily blocked due to a time zone plan you will hear a single signal tone; however, the cylinder will not engage so that the internal or external knob remains freely rotatable and the door firmly locked.

1.5 Opening and locking from the inside

The door can only be opened or locked from the inside using the transponder. The exception to this rule is the locking cylinder type .TS (keypad control) which can be engaged mechanically from the inside. This model allows the door to be opened and locked from the inside without the use of an authorised transponder. Doors with this model are not entered into the access list.

2. Versions

The digital locking cylinder 3061 is available in the following versions:

2.1 Standard version

The standard version is a locking cylinder that is freely rotatable on both sides with Yes/No authorisation. The cylinder can differentiate between a maximum of 8,187 different transponder IDs (TIDs). The cylinder complies with IP Class 54 when fitted, but its actuator must be protected against contact with water.

2.2 ZK version

Same design as the standard version but with access logging and time zone control.

Access logging	The locking cylinder can log the last 3,072 admissions together with the corresponding date, time and transponder ID (TID). The data is retrievable at any time using the programming device or via the network.
Time zone control	Locking cylinders can be programmed to grant access to authorised transponders only at specific times. Each locking system can handle a maximum of 16,383 different time zone plans and 5(+1) different time zone groups for each locking action.

2.3 FH version

Same design as the standard version but for doors with strong metal inserts (fire doors) or with greater shielding effectiveness. This version is recommended for use in areas with strong fields of interference, for instance in server rooms and for all metal doors. The FH version cannot be retrofitted.
This cylinder version is recommended for networked locking cylinders as it makes project planning easier.

2.4 TS version

Same design as the standard version but with the additional option of engaging the cylinder from the inside without the use of a transponder. Two buttons on the internal knob allow this cylinder version to be engaged mechanically. In other words, the door can be operated from the inside without the use of a transponder. The cylinder engages for approx. 5 seconds, allowing the door to be opened or locked. The cylinder rotates freely again after the time period has lapsed.
The .TS version cannot be retrofitted.

2.5 MS version

Locking cylinder 3061 is also available in brass (high gloss) as an alternative to stainless steel.

2.6 VdS version

Locking cylinder 3061 is also available as a VdS cylinder. Additional mechanical protection places this version in VdS Class B. This version cannot be combined with the WP and anti-panic versions. The VdS cylinder is only available in combination with ZK functionality.

Note: profile cylinders on doors susceptible to breaking and entering must be protected by a VdS-approved doorplate of Class B or C. These doorplates comply with standard DIN 18 257 Class ES 2 or ES 3.

2.7 AP version

A cylinder with an anti-panic function must be fitted to all doors whose anti-panic lock functionality is influenced by the position of the actuator. This version has a lock bit with a defined position, which is why a panic lock cannot be blocked.
In contrast to all other cylinders, the cylinder type .AP is installed mirror-inverted, i.e. the knob with the batteries and electronics is located on the outside of the door (see illustration).
Contrary to standard anti-panic cylinders where the internal knob is permanently engaged, the internal knob of the freely rotating .AP version is mechanically disengaged and cannot be engaged by means of a transponder.

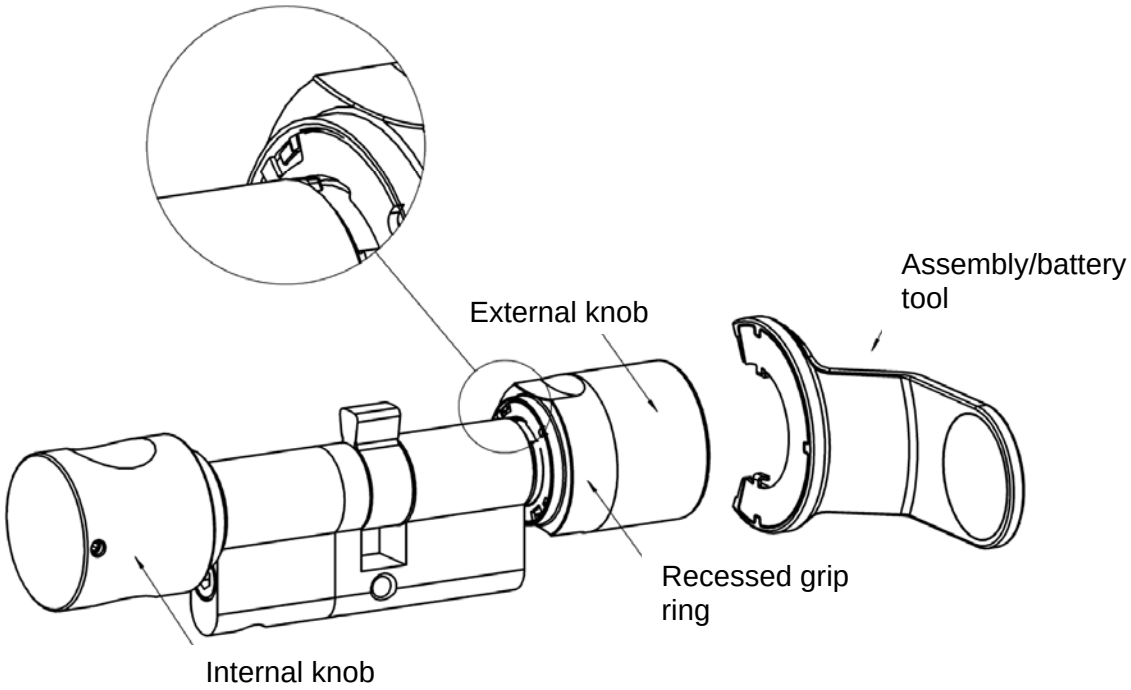


Illustration of a Type .AP cylinder

The following points need to be considered for doors installed along escape routes after 1. April 2003 (locks pursuant to standards DIN EN 179 and DIN EN 1125):

- Cylinders from the 3061 design range can be used for all locks whose approval for use states that the locking cylinder has no influence on the lock's functionality.
- Cylinders from the 3061 Type .AP (anti-panic cylinder) design range must be used for all locks where the lock functionality is influenced by the position of the locking cylinder's actuator; the cylinder must also be listed in the manufacturer's approval.

Caution: The specific design of panic locks means that it is not permissible to turn the knob of the locking cylinder up to the stop when the door is closed as this could affect the lock's panic function.

2.8 WP version

Standard cylinder: use the WP version when the electronics side of the door is located on the outside, i.e. when the knob containing the electronics is exposed to rain, for instance. The cylinder complies with IP Class 65 on account of seals and other design measures.

The WP version is designed specifically for outdoor use and should be installed if the knob can come into contact with water (e.g. rainwater). Although the WP version has a greater resistance to water, the actuator should never come into contact with it.

2.9 Overlengths

All twin-knob cylinders are available up to a maximum length of 140 mm, or 90 mm on one side. Longer versions are available on request.

2.10 Overview

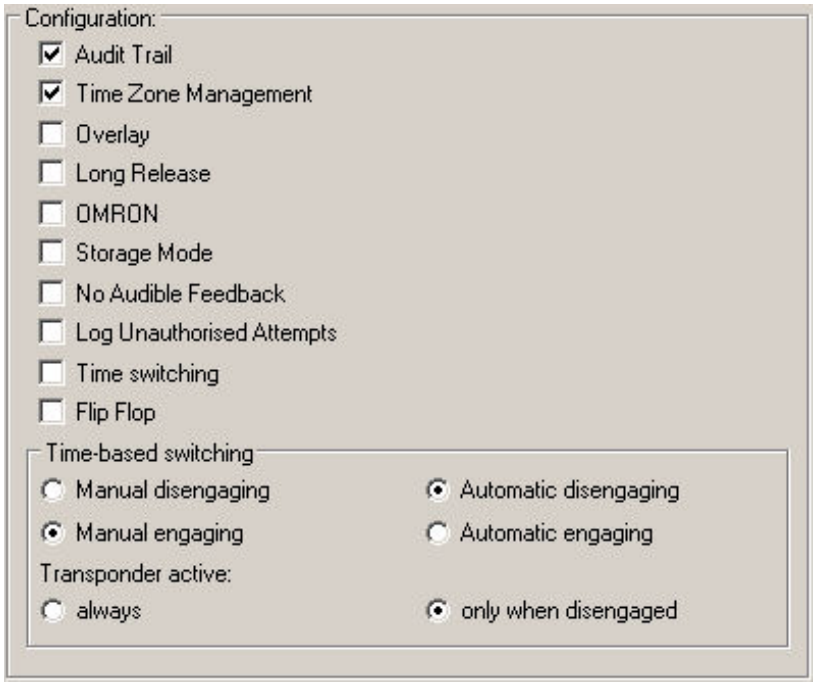
Locking cylinder (ZK)	Locking cylinder FH (ZK)	Locking cylinder TS (ZK)	Locking cylinder AP (ZK)
➢ Entrance doors	➢ Fire doors	➢ House doors	➢ Anti-panic doors [*1]
➢ House doors	➢ Aluminium doors	➢ Office doors	➢ Emergency exits [*1]
➢ Office doors			
➢ Intermediate doors			
➢ Self-locking doors			

[*1] See also chapters 2.7 and 9.3, standards EN 179 and EN 1125, and data sheets provided by lock manufacturers.

The various versions are all combinable with each other unless indicated otherwise in their respective descriptions.

3. Programming and configuration

The following configuration options are available when the locking cylinder is selected as the locking type in the SimonsVoss Software (as of LDB Version 1.52 / 1.53):



Configuration menu

3.1 Access Control

This is only possible with the .ZK version. Each of the last 3,072 transponder activations are logged by the lock with date, time and transponder ID (TID).

3.2 Time zone control

This is only possible with the .ZK version. It is possible to load time zones which then authorise and block transponders according to their time zone group.
A time zone plan also enables time-controlled switching.

3.3 Overlay mode

This mode applies to the complete locking system and needs to be selected during the system's design phase. Replacement transponders can overwrite the original transponders. The first use of a replacement transponder will overwrite and block the original transponder.

3.4 Extended activation

The cylinder's external or internal knob will engage for approx. 5 seconds as a default value. The software allows the time to be extended to 10 seconds. This does not shorten the battery life.

3.5 OMRON

Every product version is operable in OMRON mode. You should select this option for both the Smart Relay and the cylinder if you want the Smart Relay to transmit transponder data to a different system and subsequently send a remote opening command to a cylinder on approval by the other system.

Attention: Cylinders using this configuration cannot be opened by a transponder.

Please refer to the "Smart Relay" manual for a detailed description.

3.6 Warehouse mode

Locking cylinders are delivered in warehouse mode to preserve battery power. Locking cylinders in warehouse mode cannot be addressed by a transponder. The warehouse mode is deactivated when the locking cylinder is programmed for the first time. It is also possible to deactivate the warehouse mode using the programming software without creating a locking plan.

For warehouse mode after battery warning level 2: see chapter 6.

3.7 No acoustic confirmation signals

This checkbox should be activated if you want to suppress the acoustic confirmation signal for programming from the locking cylinder.

This function is especially practical for network-based programming or data reading, as the acoustic signal emitted by the locking cylinder is not usually audible due to the distance.

3.8 Logging unauthorised access attempts

As a rule, the system only logs authorised transponder operations. You will need to select this option if you wish to log attempts to open the door using an unauthorised transponder.

Unauthorised access attempts include:

- Access attempts without authorisation
- Access attempts outside of the authorised time zone
- Access attempts under activated alarm system and simultaneous use of a SimonsVoss shunt lock.

As a general rule the system only logs transponders belonging to the same locking system, i.e. they must have the same locking system ID (SID).

3.9 Time-switch function

This is only possible with the .ZK version. The time-switch function requires a time zone plan to be loaded which then activates (engages) the locking cylinder during the specified times (in Group 5 - Locking). A door can be freely accessible by turning the knob during the day, but only accessible by means of transponder during the night. Caution: The lock does not engage automatically when the knob is disengaged.

The following options are available in the field "Time-controlled activation" when the time-switch function is selected:

1. Manual disengage
   The locking cylinder does not disengage automatically at the appointed time but remains engaged until a subsequent command is received from an authorised transponder.

2. Automatic disengage (default setting)
   The locking cylinder disengages automatically at the time appointed in the time zone plan.

3. Manual engage (default setting)
   The locking cylinder does not engage automatically at the appointed time but remains disengaged until a subsequent command is received from an authorised transponder.

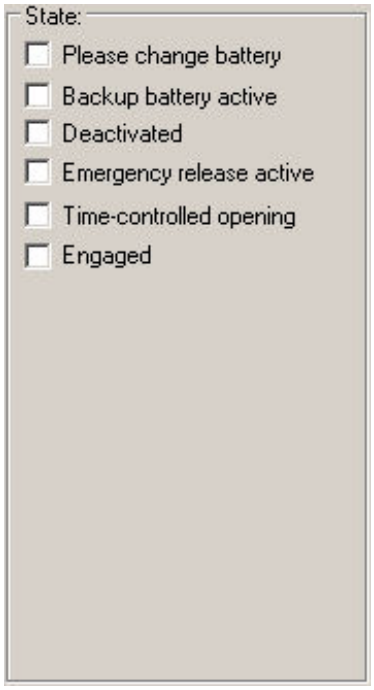
4. Automatic engage
   The locking cylinder does not engage automatically at the appointed time but remains disengaged until a subsequent command is received from the first transponder. You should select this option of you want the locking cylinder to engage automatically at the appointed time.

5. Transponder active
   - Always
     Transponders cannot usually be used when the door is freely accessible. However, you should select this option if you want to be able to lock a freely accessible door (for instance if everyone has left the building). In other words, if you want to manually override the time-switch.
   - Only when locked
     In this mode the transponder will not work during the general access period, i.e. when the cylinder is engaged.

3.10 Flip-Flop

Deactivates the pulse mode (default setting), the pulse length is no longer relevant. When in flip-flop mode the locking cylinder will change its status from engaged to disengaged or vice versa whenever a transponder is operated. This mode is recommendable if, for instance, you want to make a door freely accessible without the use of a transponder.

4. Status reports



Status menu

4.1 Battery condition critical

This checkbox is checked automatically by the programming software when battery capacity starts to decline and status changes to battery warning level 1. Please change the batteries.

4.2 Emergency battery activated

The locking cylinder will automatically change to battery warning level 2 if battery capacity continues to decline and the previous warning remains unheeded. The checkbox under item 4.1 is checked automatically by the programming software.
A battery change is now imperative.
The cylinder will automatically switch to the emergency battery - warehouse mode after around 50 operations or approximately 4 weeks (see chapter 6 Battery warnings).

4.3 Deactivated

This checkbox is automatically checked by the programming software if the locking cylinder was deactivated via a SimonsVoss shunt lock or the SimonsVoss network.

4.4 Emergency connection activated

Locking cylinders installed within a SimonsVoss network can be permanently engaged automatically via an automated command in the programming software. The signal is usually transmitted by a fire detection system and can be interpreted by the LDB (if configured accordingly).

4.5 Time-controlled opening active

This box is checked if the time-switch function has been programmed and the locking cylinder engaged automatically by the time switch.

4.6 Engaged

This box is checked if the time-switch function or flip-flop mode has been programmed and the locking cylinder is engaged.

5. Installation instructions

5.1 General notes

When installing the digital locking cylinder, make sure no sources of low-frequency radio interference are located nearby. There should be at least 0.5 m distance between individual locking cylinders and 1.5 m between Smart Relays or arming units.

The profile cylinder housing of the locking cylinder must not protrude more than 3 mm on the outside; use a profile cylinder collar where necessary. It is also imperative that no water can enter the cylinder through the actuator area.

Do not strike or hit the knobs under any circumstances during installation.

Both knobs are closed by means of bayonet locks (exception: internal anti-panic version).

The inside part of the locking cylinder is identifiable by a sticker (IL for inside length) on the profile cylinder housing, and also by the black plastic ring located between the internal knob and the profile cylinder housing.

Batteries are already installed in the unit on delivery.

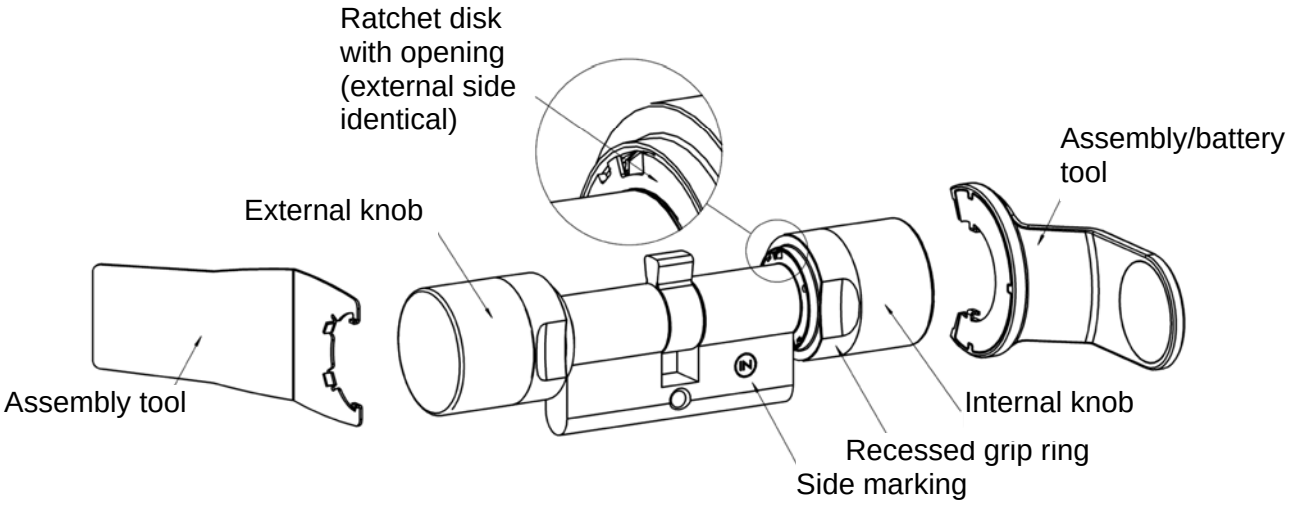
The installation work described in this chapter can only be executed with the installation/battery tool.

5.2 Programming the locking cylinder

The digital locking cylinder and the corresponding transponders must be programmed into the locking plan prior to installation. Please see the software operating instructions for further details.

- Locking cylinders are delivered from the factory in so-called warehouse mode; communication with transponders is not possible in this mode (exception: programming transponder). You can also deactivate warehouse mode using the software and the programming device; please refer to the software instructions for further details.

5.3 Installing twin-knob cylinders (except Type .AP)



5.3.1 Remove the external knob

Hold the assembly/battery tool against the external knob so that both nibs fit into the openings on the external knob (if necessary rotate the knob until the nibs slot into the ratchet disk).

Attention: The assembly tool must be held flush against the face of the knob to fit properly into the ratchet disk.

Hold the knob and carefully turn the assembly/battery tool 30° in a clockwise direction (until you hear a clicking noise). Remove the knob.

5.3.2 Fitting the digital cylinder in the lock

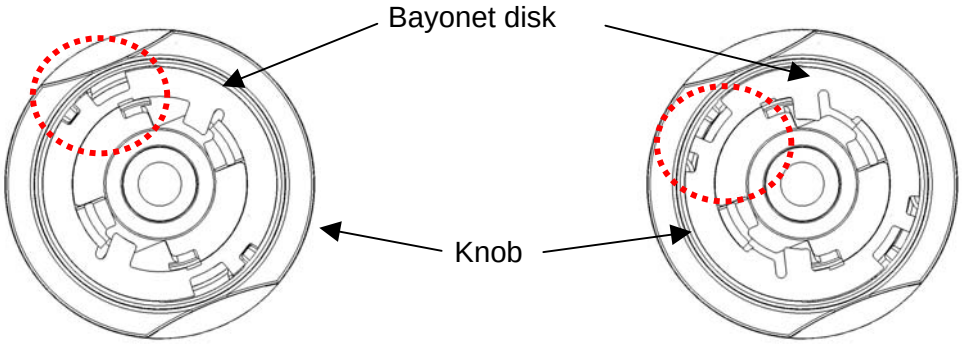
Turn the actuator until it is vertical and pointing downwards. Push the digital locking cylinder through the lock so that the internal knob (see illustration in chapter 5.3) is facing the inside surface of the door. Secure the locking cylinder in the slot-in lock with the fixing screw.

- Do not strike or hit the knobs under any circumstances during installation. The cylinder must not come into contact with oil, paint or acids.

5.3.3 Fitting the external knob

Replace the knob and rotate it anti-clockwise under light pressure until the external knob fits into the recesses on the flange. If necessary, push the knob in this position towards the profile cylinder housing.

Caution: rotating the bayonet disk when not installed can prevent the knob from fitting correctly. In this case use the assembly tool to turn the bayonet disk back to the original "bayonet disk open" position. (See illustrations)



Bayonet disk closed Bayonet disk open

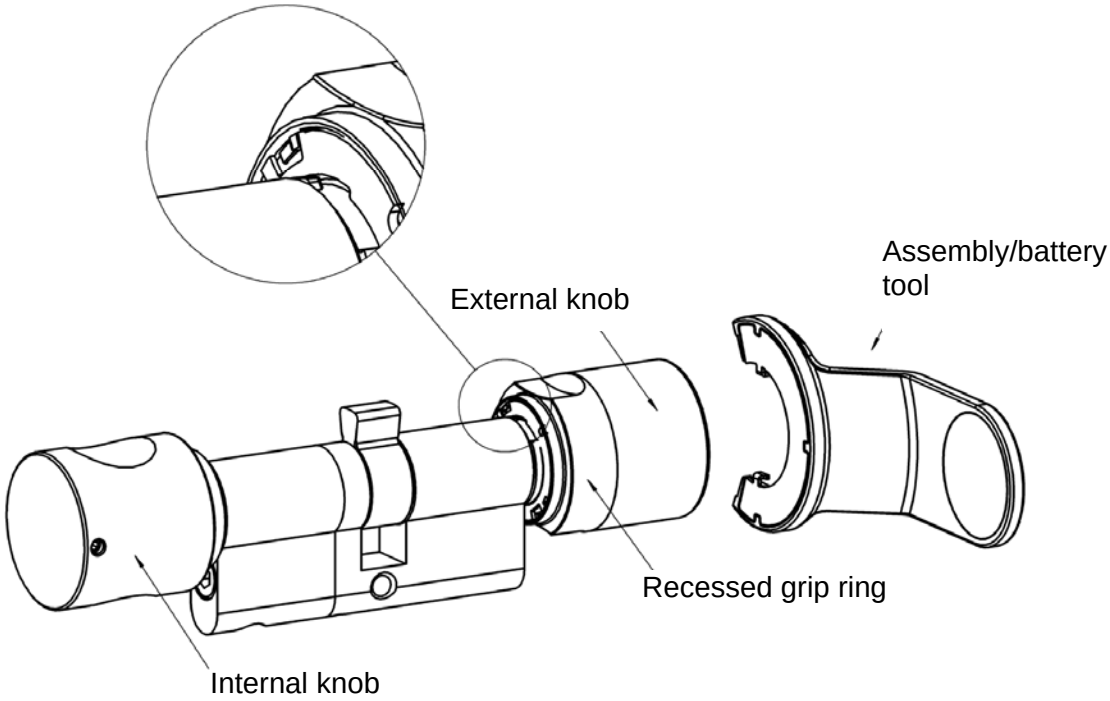
Hold the assembly tool so that the two nibs fit into the external knob (if necessary, turn the knob until the two nibs hook into the recesses). Rotate the knob clockwise by 30° to close it again.

5.3.4 Perform a function test

1. Engage the locking cylinder using the transponder; with the door open, rotate the *knob* in both directions for opening and locking. The knob should rotate easily in both directions.

2. Close the door and repeat the test. If the knob is difficult to rotate you will need to adjust the door or the striking plate.

5.4 Installing the anti-panic cylinder (Type .AP)



5.4.1 Remove internal knob

Loosen the inner knob's threaded pin (see illustration in chapter 5.4) with an Allen key (but do not unscrew it completely). Hold the actuator and then screw off the internal knob in an anti-clockwise direction, or pull the knob from freely rotating .AP cylinders after loosening the threaded pin.

5.4.2 Securing the digital cylinder in the lock

First turn the actuator until it is vertical and pointing downwards. Push the digital locking cylinder through the lock from the outside so that the external knob (see illustration in chapter 5.4) is facing towards the outside of the door. Secure the locking cylinder in the slot-in lock with the fixing screw.

- Do not strike or hit the knobs under any circumstances during installation. The cylinder must not come into contact with oil, paint or acids.

5.4.3 Fitting the internal knob

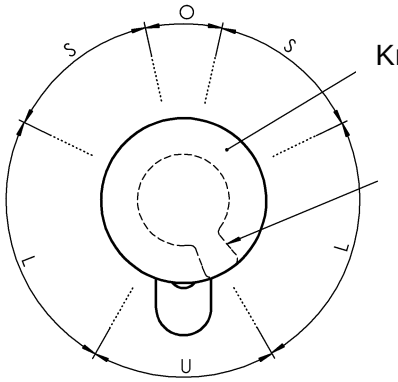
Screw the *internal knob* onto the thread; the actuator in the lock will provide the necessary counterforce. Tighten the *inner knob* or, in the case of .AP cylinders, slide it right up to the stop. Tighten the *threaded pin* with the Allen key.

5.4.4 Perform a function test

- The test can be performed from the inside for anti-panic cylinders that do not rotate freely; the test must be performed from the outside with an authorised transponder for freely rotating anti-panic cylinders.

- The internal knob of freely rotating .AP cylinders has no function whatsoever.

Area U: lower area without reset force
Area L: slight reset force
Area S: strong reset force
Area O: upper area without reset force



1. With the door open turn the *internal knob* (see illustration in chapter 5.4) in both directions within the area marked "U": you will not feel any reset force.

2. Turn the internal knob to the end of the area marked "L": you should feel a slight reset force. If you let go of the internal knob in this position it should move back to the "U" area of its own accord.
   Otherwise realign the locking cylinder and fittings or check the lock for defects.

3. Now rotate the knob through the area marked "S" (you will notice a distinct increase in reset force) to the area marked "O". Reset force does not have any effect in this area.

- Actuators that remain in the highest position will have no effect on the functionality of approved anti-panic locks pursuant to standards DIN EN 179 and DIN EN 1125.

4. If the knob is moved slightly beyond the transition point between the areas "O" and "S" it must continue to rotate of its own accord until it reaches to the area marked "U".
   Otherwise realign the locking cylinder and fittings or check the lock for defects.

5. Close the door and repeat the test. If the knob is difficult to rotate you will need to adjust the door or the striking plate.

6. Then check the same functionality on the *external knob* after activating the knob with an authorised transponder (see illustration in chapter 5.4).

The functionality test must be carried out for both directions of rotation.

Note: European standard EN 179 Appendix C recommends that all lock components should be checked for satisfactory functionality during emergency exit locks maintenance checks at regular intervals of no more than one month.

6. Battery warnings

Each locking cylinder has a battery management system that indicates declining battery power in good time. This helps prevent the batteries from becoming completely discharged. The battery warning levels are described in the following.

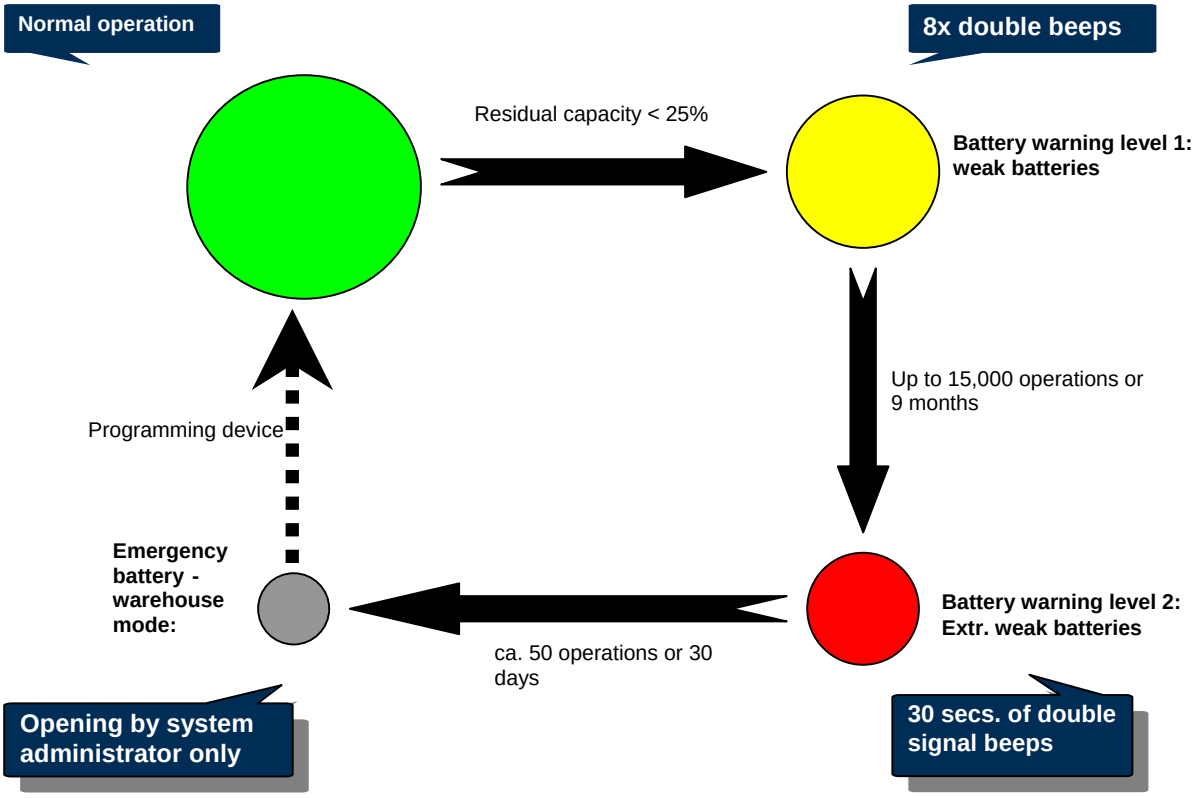
6.1 Locking cylinder

Warning level 1: weak batteries
When a locking cylinder's batteries are running low it will emit eight short signal tones in rapid succession when operated by a transponder before the locking cylinder engages. The batteries should be replaced without delay. Around 15,000 opening or 9 months use of the locking cylinder remain after battery warning 1 has been triggered.

Warning level 2: extremely weak batteries
If the batteries are allowed to discharge even further, subsequent transponder operation will induce a succession of short signal tones lasting approximately 30 seconds before the cylinder engages. The cylinder will not engage until after the acoustic signal has ended. The batteries are now virtually completely discharged. It is imperative they are replaced as soon as possible.

Emergency battery - warehouse mode:
A locking cylinder that has indicated battery warning level 2 will remain active for approximately another 50 operations, or it will shut down completely after approximately 30 days if not used. In both cases the locking cylinder will revert back to the so-called emergency battery - warehouse mode. The locking cylinder can now only engage with the help of a programming device (see chapter 6.1.3).

6.1.1 Schema


Normal operation
8x double beeps
Residual capacity < 25%
Battery warning level 1: weak batteries
Up to 15,000 operations or 9 months
Programming device
Emergency battery - warehouse mode:
Battery warning level 2: Extr. weak batteries
ca. 50 operations or 30 days
Opening by system administrator only
30 secs. of double signal beeps

6.1.2 Procedure for emergency battery - warehouse mode

Please proceed as follows to change the batteries if the locking cylinder is in emergency battery - warehouse mode:

- Go to the door and take a Notebook or PDA (having exported the locking plan) and a programming device with you.
- Select the appropriate locking from the locking plan.
- Program over the cylinder once without making any changes. This deactivates the two battery warning check boxes and the warehouse mode.
- Use an authorised transponder to engage the locking cylinder and then open the door. (The locking cylinder will immediately revert back to warehouse mode as both batteries are virtually empty).
- Replacing batteries (see chapter Battery change).
- Program over the cylinder once without making any changes. This deactivates the two battery warning check boxes and the warehouse mode.
- Use the authorised transponder to engage the locking cylinder.

The locking cylinder will emit the level 2 battery warning once more after the batteries have been changed. The locking cylinder's electronic system will then detect that the batteries are at full capacity or have been replaced and the locking cylinder will work as normal.

This procedure is only necessary in the emergency battery - warehouse mode condition. This mode was introduced to prevent the batteries from completely discharging without intervention by the locking system administrator. Nonetheless, batteries in emergency battery - warehouse mode should be changed as soon as possible.

6.2 Transponder

When the transponder's battery voltage starts to decline, each operation will cause the locking cylinder to emit eight short signal tones in rapid succession after it has disengaged.

7. Signal tones

Signal type	Meaning	Required action
2 short tones prior to engaging and one short tone after disengaging	Normal operation	None
Battery warning level 1: 8 short tones prior to engaging	Batteries will soon be empty	Change the cylinder batteries
Battery warning level 2: **8 short tones for 30 seconds with a one-second break between each set**	Batteries are nearly completely discharged	**Replace the cylinder batteries immediately!**
8 short tones after disengaging	Transponder battery empty	Have the transponder battery changed
1 short signal tone without engaging the cylinder	• Attempt to operate outside of time zone • Armed alarm system with simultaneous use of a SimonsVoss shunt lock	None

8. Battery change

8.1 General notes

Batteries should only be changed by trained personnel. Only use batteries approved by SimonsVoss.
On anti-panic cylinders these steps should be carried out on the external knob as the batteries and electronics are located on the external side.
Please see the data sheet for further information.

Reversing polarity can result in damage to the locking cylinder. The batteries used in this device can cause fire or burns if handled incorrectly. Do not charge, open, heat above 100°C, short-circuit or burn batteries.

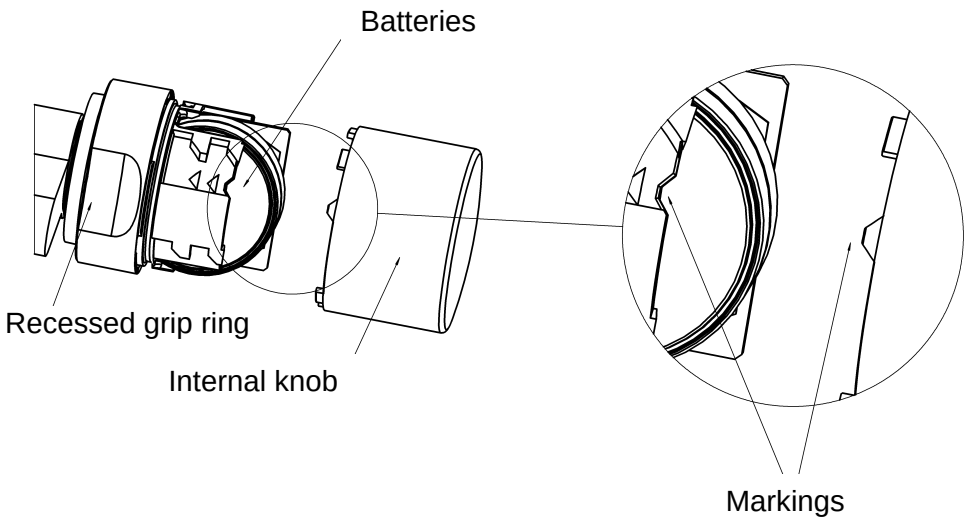
- Please dispose of discharged lithium batteries immediately. Keep out of reach of children. Do not open. Do not throw into a fire.

Always replace both batteries together at the same time.

Please also see the safety notes in chapter 1.1.

8.2 Procedure

1. Hold the assembly/battery tool against the knob so that both nibs fit into the openings on the ratchet disk (if necessary rotate the knob until the nibs slot into the openings).
   Attention: The assembly/battery tool must be held flush against the inner surface of the recessed grip ring to fit into the ratchet disk.
2. Hold the knob and carefully turn the assembly/battery tool 30° in a clockwise direction (until you hear a clicking noise).
3. Remove the assembly/battery tool from the knob.
4. Slide the recessed grip ring back towards the door until it slips off the knob.
5. Hold the recessed grip ring, rotate the knob approx. 10° anti-clockwise and remove.
6. Carefully remove both batteries from their bracket.
7. Hold the two new batteries with plus poles facing each other and slide them into the bracket (please replace the batteries as quickly as possible). Make sure you wear clean, grease-free gloves when handling new batteries.



8. Replace the knob (according to the triangular markings, see drawing), hold the recessed grip ring and rotate the inner knob (approx. 10°) in a clockwise direction to tighten.

9. Slide the recessed grip ring back onto the knob so that the knob and ring are flush against each other.
10. Hold the assembly/battery tool against the internal knob so that both nibs fit into the openings on the ratchet disk (if necessary rotate the knob until the nibs slot into the openings).
11. Lock the knob by rotating it approx. 30° in a clockwise direction (until you hear a clicking noise).

Use an authorised transponder to check functionality.

👍 When replacing the batteries on a ZK version you may have to reset the time as the clock will stop running when the power supply is interrupted (software operating instructions: Programming → Set locking clock time).

9. Possible uses

9.1 General

The digital locking cylinder is designed to fit locks for Euro profile cylinders compliant with DIN 18252 and EN1303.

9.2 Fire doors

Installation in fire doors is possible. The locking cylinder version FH should be used for these doors and for metal doors.

9.3 Doors on escape routes

The .AP model should be installed in anti-panic doors where the position of the actuator can influence the functionality of the lock. The model must be approved for use by the lock manufacturer. See also chapter 2.4, standards DIN EN 179 and DIN EN 1125 and the product data sheets provided by each lock manufacturer.

9.4 Outdoor installation situations

Unless it is ensured that the door is completely water-proof it is recommendable to use the .WP version of each respective model. The external knob on anti-panic cylinders is completely sealed; the entire cylinder is completely sealed on the twin-knob cylinder version.

10. Accessories

10.1 Knobs

The following special knobs are available as accessories:

- External knob in a TN3 design
- External knob 42 mm diameter with grip recesses
- Internal knob 36 mm diameter for .TS cylinders
- External knob shortened
- Brass knob matt (internal and external knobs)

These knobs can be used to replace the original locking cylinder knobs at any time. For knob installation see chapter 5 (installation instructions) or chapter 7 (battery change).

10.2 Core protection adapter set

A mechanical extension is available for core protection hardware as the profiles on these is not machined out. The extension is 8 mm in length and be retrofitted at any time.

10.3 Tools

An assembly/battery tool is supplied in addition to the installation tools. This tool is used to assemble and disassemble the external knobs and to replace batteries.

10.4 Battery set

Battery packs are available to order. This set contains 10 batteries of type CR2450. Please only use batteries approved by SimonsVoss.

11. Data sheet

Knobs	Material Colours Diameter Length	Stainless steel Satin stainless steel 30 mm 37 mm (from profile face)
FH cylinder knobs	Material Colours Diameter Length	Internal knob: cap stainless steel Recessed grip area plastic External knob: identical to standard cyl. Cap: satin stainless steel Recessed grip area black External knob identical to standard cyl. 30 mm 37 mm (from profile face)
AP cylinder knobs	Material Colour Diameter Length	External knob: identical to standard cyl. Internal knob: Aluminium External knob: satin stainless steel Internal knob: nickel-plated aluminium 30 mm External 37 mm (from profile face) Internal: ca. 36 mm (from profile face)
AP cylinder knobs	Material Colour Diameter Length	External knob: identical to standard cyl. Internal knob: identical to standard cyl. External knob: Cap: gloss brass Recessed grip area: matt brass Internal knob: Cap: brass gloss Recessed grip area: brass matt 30 mm 37 mm (from profile face)
Profile cylinder	Basic length	External 30 mm, internal 30 mm Design lengths in increments of 5 mm (no kits) up to an overall length of 140 mm whereby one side of the cylinder can have a maximum length of 90 mm. Longer lengths available on request.
Profile cylinder AP / WP	Basic length	External 30 mm, internal 35 mm Design lengths in increments of 5 mm (no kits) up to an overall length of 140 mm whereby one side of the cylinder can have a maximum length of 90 mm. Longer lengths available on request.

Batteries	Type	CR 2450
	Manufacturer	Varta, (Panasonic, Sony)
	Quantity	2 pieces
	Voltage	3 Volt
	Lifetime	Approx. 150,000 operations or approx. 7 years on stand-by
Ambient conditions		
	Operating temperature	-20°C to +50°C
	Storage temperature	-30°C to +60°C
	Protection Class	IP 54 (when installed) Variant .WP: IP 65

Digital Half Cylinder 3061

State of: September 2006

SimonsVoss technologies

Digital Half Cylinder 3061

Content

1.0 Method of Operation ____ 4
1.1 General Information ____ 4
1.2 Opening and Locking ____ 4
2.0 Special Models ____ 4
2.1 PLUS Version ____ 4
3.0 Additional Functions ____ 5
3.1 OMRON ____ 5
3.2 Extending the Coupling Time ____ 5
3.3 Logging Unauthorized Access Attempts ____ 5
3.4 No Acoustic Programmer Acknowledge ____ 5
4.0 Battery Warnings ____ 6
4.1 Half Cylinder ____ 6
4.2 Transponder ____ 6
5.0 Battery Replacement ____ 7

Content

6.0 Installation Instructions 8
6.1 General Information 8
6.2 Programming a Half Cylinder 8
6.3 Installing in Doors 8
6.4 Installation Behind Blanks for Half Cylinders With 3 Setscrews 9
(New Flange Mounting) 9
6.4.1 Removal of the Knob and Flange of the Half Cylinder 9
6.4.2 Installing the Knob and Flange of the Half Cylinder 10
6.5 Installation Behind Blanks for Half Cylinders With 2 Setscrews 11
(Old Flange Mounting) 11
6.5.1 Removal of the Knob and Flange of the Half Cylinder 11
6.5.2 Installing the Knob and Flange of the Half Cylinder 11
6.6 Perform Function Test 12
7.0 Data Sheet 13

1.0 Method of Operation

1.0 General Information

The outer dimensions of the Digital Half Cylinder exactly match those of a mechanical cylinder complying with DIN 18252. Please ask for approved self-locking and anti-panic locks at the manufacturer.

1.1 Opening and Locking

When not activated, the outer knob turns freely. It is not possible to open the door or to lock it. Hold the transponder at a distance of approximately 10 to 40 cm (4 to 16 inches) from the digital half cylinder and briefly press the transponder button once. If this is an authorised transponder, a double signal tone sounds and the cylinder couples. Now turn the outer knob in the locking or opening direction. You have approximately five seconds for this process. Then a single signal tone sounds and the outer knob turns freely again. Make sure that the outer knob of the half cylinder turns freely again after the coupling process.

- If this is a transponder that is not authorised at this time because of the time zone plan, a single signal tone sounds. The cylinder does not couple, however, and you cannot open the door.

2.0 Special Models

The Digital Half Cylinder 3061 is also available in the following optional versions:

2.0 PLUS Version

Design is similar to the standard version but with access logging and time zone control.

Access logging	The locking cylinder stores the last 128 accesses with date, time and the user name of the transponder. You can read out the data with the SmartCD or over the network.
Time zone control	You can program locking cylinders in such a way that authorised transponders are authorised for access only at certain times.
Weatherproof	This version is also approved for outdoor use. The knob is certified to IP 65.
Multi-ratchet	A spring mechanism (with 8 ratchet-points) prevents the key tab from turning with the knob when not coupled (e.g. for use in key-switches).

3.0 Additional Functions

3.1 OMRON

All product versions can be operated in OMRON mode. You will find a detailed description in the Smart Relay manual.

3.2 Extending the Coupling Time

The default time for the coupling of the cylinder is approximately 5 seconds. You can use the software to extend this time to approximately 10 seconds. This shortens the lifetime of the battery, however.

3.3 Logging Unauthorised Access Attempts

For cylinder version 10.2 and later and in combination with the LDB Version 1.40 and later, it is possible to log unauthorised access attempts, as well as authorised accesses. This includes both access attempts without authorisation and
access attempts outside the specified time zone. In this connection, however, only transponders from the locking system are logged, which means that the transponder must have the same locking system ID (SID).

3.4 No Acoustic Programmer Acknowledge

When programming over the network, it can be advantageous to deactivate the acoustic programmer acknowledge. You can do that with this function.

4.0 Battery Warnings

4.1 Half Cylinder

Warning level 1 for main battery
If the main battery of the half cylinder goes empty, eight short signal tones, coming quickly one after another, sound after you operate the transponder and before the cylinder couples. You must replace both batteries now.

Warning level 2 for backup battery (SW Version 10.0 & SW Version 10.1)
In addition to the main battery warning, an additional sixteen short signal tones, coming quickly one after another, sound for the backup battery warning. The cylinder does not couple until after the signals. From now on, the backup battery is active. You must replace both batteries as soon as possible.

Warning level 2 for backup battery (SW Version 10.2 and later)
In addition to the main battery warning, the signal tones of the backup battery warning now sound for approximately 30 seconds. The cylinder does not couple until after the signals. From now on, the backup battery is active. You must replace both batteries as soon as possible.

Warning Level 3 (SW version 10.3 and later)
If you continue to ignore the backup battery warning, either the door can be used 50 more times or the cylinder switches off after ca. 4 weeks if there is no further operation. In both cases, the cylinder switches into the so-called storage mode. After this, you can only open the cylinder with the programming device.

4.2 Transponder

If the transponder battery voltage is coming to an end, eight short signal tones, coming quickly one after another, sound each time the transponder is operated and after the uncoupling. (look at manual digital-locking-cylinder 3061)

Attention: Do not take out the transponder battery because this will probably result in the loss of data. See the “Transponder 3064” manual for more information.

5.0 Battery Replacement

Only authorised personnel are permitted to replace the battery. Use only batteries that are supplied by SimonsVoss.

1. Firmly hold the knob and remove the locknut on the back of the knob from the knob with the special tool for half cylinders.
2. Use an authorised transponder to couple the cylinder and unscrew the knob by turning it counter-clockwise. While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
3. Replace the main and emergency batteries. Make sure that the polarity is correct.
4. Use an authorised transponder to couple the half cylinder and tightly screw the knob in until the stop. Make sure that the knob is screwed on up to the stop (important for the function). While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
5. Firmly hold the knob and use the special tool for half cylinders to firmly screw the locknut onto the knob.
6. Now operate an authorised transponder and test the function.

Dispose of used batteries immediately, keep out of reach of children, do not open and do not throw into a fire!

- Reversing the polarity can result in damage to the locking cylinder. Incorrect handling of the batteries used in this device can result in the risk of fire or burns. Do not charge, open, heat to more than 100° C (212° F) or burn.

- Never operate the cylinder without a main battery because otherwise the entire power consumption of the cylinder runs over the backup battery.

- For PLUS versions, you must reset the time of day after the battery change because the clock does not work without current (Software Operating Instructions: Programming → Setting the clock on the locking).

6.0 Installation Instructions

6.1 General Information

Only trained and authorised personnel are permitted to perform the installation. The battery used in the cylinder can present a risk of fire and burns if not handled correctly! Do not charge, open, heat to more than 100° C (212° F) or burn! Do not short-circuit! When installing the digital half cylinder, make sure that there are no sources of interference in the vicinity. You should install half cylinders at least 0.5 m (approximately 1.5 feet) from one another and Smart Relays or activation units at a distance of at least 1.5 m (approximately 5 feet). The PC housing of the half cylinder is not allowed to stick out into the exterior area more than 3 mm. If necessary, attach a profile cylinder rosette. Furthermore, you must ensure that no water can penetrate into the cylinder in the area of the catch.

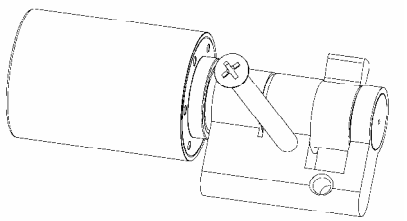
6.2 Programming a Half Cylinder

You must program the digital locking cylinder and accompanying transponders in the locking plan before you install them. Please refer to the Software Operating Instructions for more detailed information.

- The locking cylinders are delivered in so-called storage mode, which means that no communication is possible with the transponder (exception: programming transponder). You can also use software and the programming device to remove the storage mode. Please refer to the Software Operating Instructions for more detailed information.

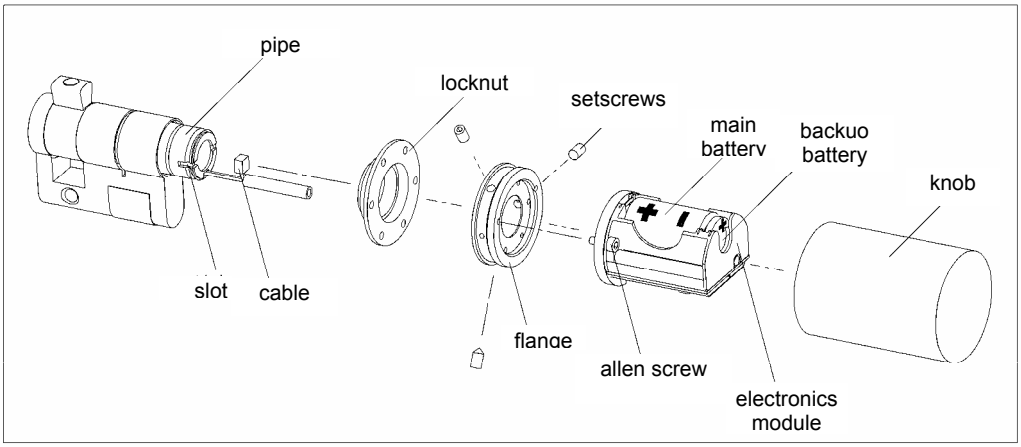
6.3 Installing in Doors

Insert the cylinder through the lock from the outside of the door towards the inside and secure it with the lock screw.



- Never hit against the knobs during installation. Do not bring the cylinder into contact with oil, paint or acid.

6.4 Installation Behind Blanks for Half Cylinders With 3 Setscrews (New Flange Mounting)



6.4.1 Removal of the Knob and Flange of the Half Cylinder

1. Firmly hold the knob and remove the locknut on the back of the knob from the knob with the special tool for half cylinders. (If the locknut is already bumping into the profile, then start to unscrew the knob as described in the following point (approximately one rotation) and continue).

2. Use an authorised transponder to couple the cylinder and then unscrew the knob. While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.

3. Carefully pull the cable out of the socket-contact in the electronics but do not remove the insulation sleeving. The electronic covering is thermally welded on and also remains on the unit.
4. Remove the two Allen screws that are parallel to the battery from the flange with an Allen key (1.5 mm). Remove the electronics module.

5. Remove the three setscrews on the outer circumference of the flange (same Allen key).
   Note: If you can see two setscrews here, this cylinder has an old flange mounting (in this case, refer to Point 6.5).

6. Remove the flange and locknut.

7. Now you can install the blank.

6.4.2 Installing the Knob and Flange of the Half Cylinder

1. Put on the locknut. The flat surface with the bore holes faces away from the cylinder.
   Note: If you cannot see any screw thread on the end of the pipe, this cylinder has a new flange mounting (in this case, refer to Point 6.4).

2. Put the flange onto the end of the pipe; the side of the flange with the screw thread faces away from the cylinder. The flange contains a crosspin that sticks out of the interior diameter. This crosspin must catch in the longitudinal slot of the pipe. Push the flange up against the stop on the pipe.

3. Holding it in this position, fix the three setscrews very tightly with the Allen key (1.5 mm). Check whether the setscrews are really tightly screwed, because this is important for correct functioning.

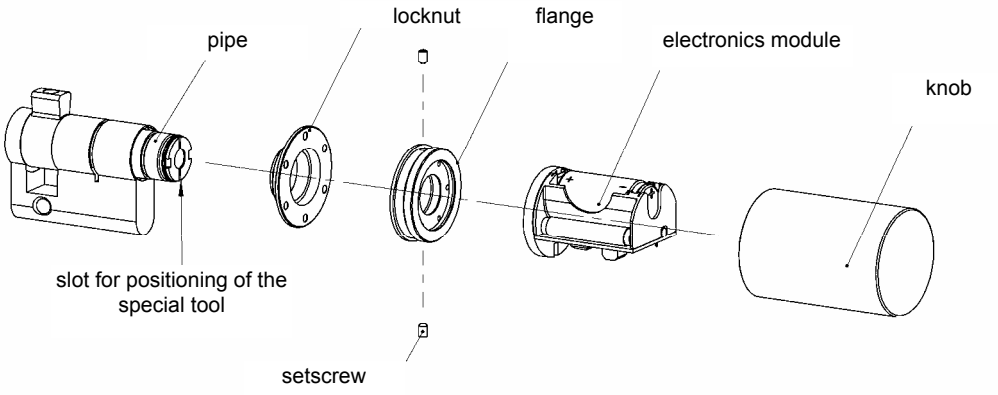
4. Fix the electronics module to the flange with the Allen screws that are parallel to the battery (same Allen key as above). Guide the cable through the recess next to the connector. Make sure that the cable is not pinched.

5. Connect the cable to the electronics socket and lay it so that it is flat on the electronics covering and not in the way when screwing on the knob (danger of pinching).

6. Use an authorised transponder to couple the half cylinder and tightly screw the knob in until the stop. Make sure that the knob is screwed on up to the stop (important for the function). While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.

7. Firmly hold the knob and use the special tool for half cylinders to firmly screw the locknut onto the knob.

6.5 Installation Behind Blanks for Half Cylinders With 2 Setscrews (Old Flange Mounting)



6.5.1 Removal of the Knob and Flange of the Half Cylinder

1. Firmly hold the knob and remove the locknut on the back of the knob from the knob with the special tool for half cylinders.
2. Use an authorised transponder to couple the cylinder and then unscrew the knob. While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
3. Carefully pull the cable out of the socket-contact in the electronics but do not remove the insulation sleeving. The electronic covering is thermally welded on and also remains on the unit.
4. Remove the two Allen screws that are parallel to the battery from the flange with an Allen key (1.5 mm). Remove the electronics module.
5. Remove the setscrew on the outer circumference of the flange (same Allen key). Note: If you can see 3 setscrews here, this cylinder has a new flange mounting (in this case, refer to Point 6.4)
6. The fore-part of the pipe, which sticks out of the profile, contains two slots on which you can position the special tool (offset 90° to the lengthwise slot which guides the cable). The narrow end of the installation tool can move into this slot. This ensures that the pipe cannot twist.
7. Now you can unscrew the flange without the pipe also turning.
8. Remove the locknut.
9. Now you can install the blank.

6.5.2 Installing the Knob and Flange of the Half Cylinder

1. Put on the locknut. The flat surface with the bore holes faces away from the door.
   Note: If you cannot see any screw thread on the end of the pipe, this cylinder has a new flange mounting (refer to Point 6.4).
2. Please note the two lateral impressions on opposite sides of the pipe. The lateral setscrews of the flange must fit into this later in order to guarantee that

the flange holds securely. To find the exact position quickly, the flat surfaces of the pipe and flange have black markings that must line up.

3. Put the flange on the end of the pipe without screwing it in. The side with the small outside diameter points towards the door. The fore-part of the pipe, which sticks out of the profile, contains two slots in which you can position the special tool (offset 90° to the lengthwise slot which guides the cable). The narrow end of the installation tool can move into this slot. This ensures that the pipe cannot twist.
4. The pipe should not turn during the following steps (see Point 3). Lightly screw on the flange until it reaches the stop and the markings line up. In this position, tighten the two setscrews with the Allen key (1.5 mm) so that they center in the indentations of the pipe. Then tighten both setscrews securely. Please check whether the setscrews are really tightly screwed, because this is important for correct functioning!
5. 5Fix the electronics module to the flange with the Allen screws that are parallel to the battery (same Allen key). Make sure that the cable is not pinched.
6. Connect the cable to the electronics socket and lay it so that it is flat on the electronics covering and not in the way when screwing on the knob (danger of pinching).
7. Use an authorised transponder to couple the half cylinder and tightly screw the knob in until the stop. While doing this, you must firmly hold the catch with your hand if the half cylinder is not installed. If the half cylinder is installed, the catch is held by the stop within the lock.
8. Firmly hold the knob and use the special tool for half cylinders to firmly screw the locknut onto the knob.

6.6 Perform Function Test

1. Operate an authorised transponder and turn the knob in the lock and open directions when the door is open. The knob must turn easily.
2. Close the door and repeat the process. If the locking cylinder is stiff, you must align the door or correct the edge plate.

7.0 Data Sheet

Dimensions	Standard length Standard length Multirast (MR) Max. profile length Knob diameter Knob length Standard for profile dimensions	30/10 mm 30/15 mm 100 mm (in 5mm intervals) 33,5 x 30 mm 51.5 mm (distance from knob end to profile fore-part) DIN 18252
Battery	Batteries Service life	Lithium, 3.6V, ½ AA, 900mAh Lithium 3V, CR1220 Use only original replacement batteries from SimonsVoss Max. 50,000 operations or roughly 4 years
Environmental Conditions	Operating temperature range Storage temperature range Degree of protection	-20°C to +50°C (-4°F to +122°F) -35°C to +50°C (-31°F to +122°F) IP 54 (when installed) IP 65 knop VW Option (when installed)

DIGITAL
HALF CYLINDER 3061

Status: April 2007

SimonsVoss technologies

1. General 4
1.1 Notes on safety 4
1.2 Product description 5
1.3 Design 5
1.4 Opening and closing 5
2. Versions 6
2.1 Standard version 6
2.2 ZK version 6
2.3 WP version 6
2.4 Overlengths 7
3. Programming and configuration 7
3.1 Access Control 7
3.2 Time zone control 8
3.3 Overlay Modus 8
3.4 Extended activation 8
3.5 OMRON 8
3.6 Warehouse mode 8
3.7 No acoustic programming confirmation 8
3.8 Logging unauthorised access attempts 9
3.9 Time-switch function 9
3.10 Flip-Flop 10
4. Status reports 11
4.1 Battery condition critical 11
4.2 Emergency battery activated 11
4.3 Deactivated 11
4.4 Emergency switch activated 12
4.5 Time-controlled opening active 12
4.6 Engaged 12
5. Installation instructions 13
5.1 General notes 13
5.2 Programming the half cylinder 13

5.3 Installing the half cylinder (except .MR) 13
5.4 Removing the multistage half cylinder 14
5.5 Installing the multistage half cylinder 15
6. Battery warnings 16
6.1 Half cylinder 16
6.2 Transponder 18
7. Signal tones 18
8. Battery change 19
8.1 General notes 19
8.2 Procedure 19
9. Possible uses 21
9.1 General 21
9.2 Outdoor installation situations 21
9.3 Key-operated switches 21
10. Accessories 21
10.1 Tool 21
10.2 Battery set 21
11. Data sheet 22

1. General

1.1 Notes on safety

- Lock installation and battery changes should only be carried out by trained personnel.
- The cylinder must not come into contact with oil, paint or acids.
- Only use batteries approved by SimonsVoss.
- The batteries used in digital locking cylinder 3061 can cause fire or burns if handled incorrectly. Do not charge, open, heat up or burn batteries. Do not short-circuit.
- Dispose of old or used batteries properly, and keep them out of the reach of children.
- Reversing polarity can result in damage to the locking cylinder.
- Always replace both batteries at the same time.
- When replacing batteries, do not touch the contact surfaces on new batteries. Always use clean, grease-free gloves.
- Cylinder operation requires two batteries.
- Use the .WP version for outdoor installations.
- SimonsVoss Technologies AG shall not be liable for damage to doors or components resulting from incorrect installation.
- An incorrectly installed or incorrectly programmed cylinder can block access through a door. SimonsVoss Technologies AG shall not be liable for any consequences of incorrect installation, such as lack of access to injured persons, material damage or other damage.
- Alterations and technical developments reserved.
- This documentation was prepared to the best of our knowledge; however errors cannot be completely ruled out. No liability is accepted in this event.
- The content of the German original shall overrule in case of differences in the content of foreign-language versions.

1.2 Product description

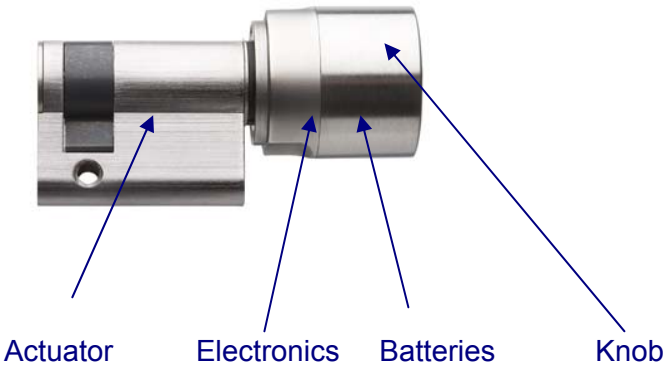
Higher security, greater flexibility, lower cost, network-capability without any wiring in doors and frames, low installation effort - all this is possible right now with the digital locking cylinder 3061. The outer dimensions of the digital locking cylinder are exactly the same as those of DIN 18254 and EN 1303; retrofitting to standard doors and locks, key-operated switches, etc., is possible at any time. It is quick and easy to exchange.

Adding new functionality to the locking cylinder's scope is made possible by upgradeable firmware. Your investment is thus protected, as "retrofitting" new functions is an uncomplicated matter.

The System 3060 has a modular design that makes it easy to install further cylinders to subsequent extensions and to manage them online as a wireless network. An integrated voltage supply makes cylinder operation self-sufficient and independent from a mains power supply. There is no need for any wiring whatsoever.

All system components are fully integratable with the SimonsVoss System 3060 due to system modularity; every SimonsVoss component is programmable using the locking plan software.

1.3 Design



1.4 Opening and closing

The knob rotates freely when deactivated. It is not possible to open or close the door or to control a key-operated switch. Hold the transponder approximately 10 to 40 cm from the digital half cylinder and briefly press the transponder button. If you are using an authorised transponder the half cylinder will emit a short double signal tone and subsequently engage. Turn the knob in the appropriate direction to lock or open the door.

You have approximately five seconds for this operation. (The engaging time can be extended to 10 seconds using the software. This will not shorten battery life.) The half cylinder will emit a single signal tone and the knob will again turn freely. Make sure the half cylinder knob turns freely after the disengaging.

If you are using a transponder that is momentarily blocked due to a time zone plan you will hear a single signal tone; however, the half cylinder will not engage so that the knob remains freely rotatable and the door firmly locked.

2. Versions

The digital half cylinder 3061 is available in the following versions:

2.1 Standard version

The standard version is a half cylinder with Yes/No authorisation. The half cylinder can differentiate between a maximum of 8,187 different transponder IDs (TIDs). The cylinder complies with IP Class 54 when fitted, but its actuator must be protected against contact with water.

2.2 ZK version

Same design as the standard version but with access logging and time zone control.

Access logging	The half cylinder can log the last 3,072 admissions together with the corresponding date, time and transponder ID (TID). The data is retrievable at any time using the programming device or via the network.
Time zone control	Half cylinders can be programmed to grant access to authorised transponders at specific times only. Each locking system can handle a maximum of 16,383 different time zone plans and 5(+1) different time zone groups for each locking action.

2.3 WP version

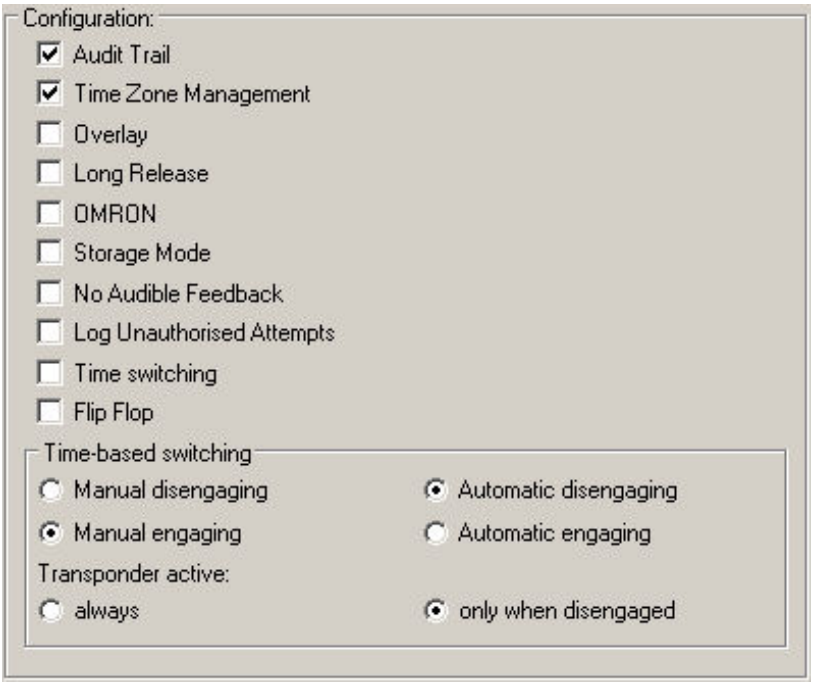
The WP version is designed specifically for outdoor use and should be installed if the knob can come into contact with water (e.g. rainwater). The WP version has a higher resistance to water, and the knob complies with IP Class 65.

2.4 Overlengths

All half cylinders are available up to a maximum length of 100 mm, and 90 mm on the external side. Longer versions are available on request.

3. Programming and configuration

The following configuration options are available when the locking cylinder is selected as the locking type in the SimonsVoss Software (as of LDB Version 1.52 / 1.53):



Configuration menu

3.1 Access Control

This is only possible with the .ZK version. Each of the last 3,072 transponder activations is logged by the lock with date, time and transponder ID (TID).

3.2 Time zone control

This is only possible with the .ZK version. It is possible to load time zones which then authorise and block transponders according to their time zone group.

A time zone plan also enables time-controlled switching.

3.3 Overlay Modus

This mode applies to the complete locking system and needs to be selected during the system's design phase. Replacement transponders can overwrite the original transponders. The first use of a replacement transponder will overwrite and block the original transponder.

3.4 Extended activation

The half cylinder engages the knob for approx. 5 seconds as standard. The software allows the time to be extended to 10 seconds. This does not shorten the battery life.

3.5 OMRON

Every product version is operable in OMRON mode. You should select this option for both the Smart Relay and the cylinder if you want the Smart Relay to transmit transponder data to a different system and subsequently send a remote opening command to a half cylinder on approval by the other system.

Attention: Cylinders using this configuration cannot be opened by a transponder.

Please refer to the "Smart Relay" manual for a detailed description.

3.6 Warehouse mode

Half cylinders are delivered in warehouse mode to preserve battery power. Half cylinders in warehouse mode cannot be addressed by a transponder. The warehouse mode is deactivated when the half cylinder is programmed for the first time. It is also possible to deactivate the warehouse mode using the programming software without creating a locking plan.

For warehouse mode after battery warning level 2: see chapter 6.

3.7 No acoustic programming confirmation

This checkbox should be activated if you want to suppress the acoustic confirmation signal for programming or reading data from the half cylinder.

This function is especially practical for network-based programming or data reading, as the acoustic signal emitted by the half cylinder is not usually audible due to the distance.

3.8 Logging unauthorised access attempts

As a rule, the system only logs authorised transponder operations. You will need to select this option if you wish to log attempts to open the door using an unauthorised transponder.

Unauthorised access attempts include:

- Access attempts without authorisation
- Access attempts outside of the authorised time zone
- Access attempts under activated alarm system and simultaneous use of a SimonsVoss shunt lock.

As a general rule the system only logs transponders belonging to the same locking system, i.e. they must have the same locking system ID (SID).

3.9 Time-switch function

This is only possible with the .ZK version. The time-switch function requires a time zone plan to be loaded which then activates the half cylinder during the specified times (in Group 5 - Locking). For instance, a door could be freely accessible during the day but only accessible via transponder at night.

Caution: The lock is not activated automatically when the knob is disengaged.

The following options are available in the field "Time-controlled activation" when the time-switch function is selected:

1. Manual disengage
   The half cylinder does not disengage automatically at the appointed time but remains engaged until a subsequent command is received from an authorised transponder.

2. Automatic disengage (default setting)
   The half cylinder disengages automatically at the time appointed in the time zone plan.

3. Manual engage (default setting)
   The half cylinder does not engage automatically at the appointed time but remains disengaged until a subsequent command is received from an authorised transponder.

4. Automatic engage

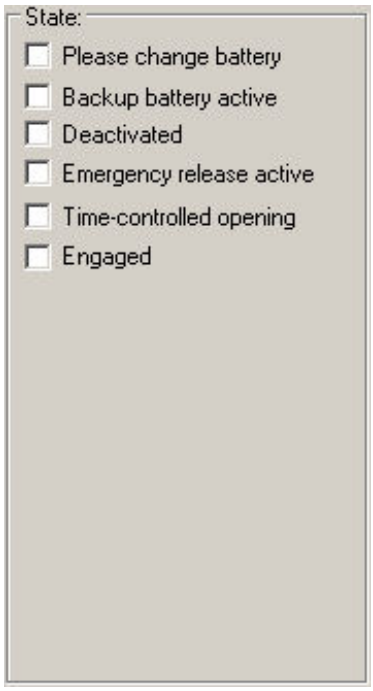
The half cylinder does not engage automatically at the appointed time but remains disengaged until a subsequent command is received from the first transponder. You should select this option if you want the half cylinder to engage automatically at the appointed time.

5. Transponder active
   - Always
     Transponders cannot usually be used when the door is freely accessible. However, you should select this option if you want to be able to lock a freely accessible door (for instance if everyone has left the building). In other words, if you want to manually override the time-switch.
   - Only when locked
     This mode renders transponders unable to operate a freely accessible door during the general access period.

3.10 Flip-Flop

Deactivates the pulse mode (default setting), the pulse length is no longer relevant. When in flip-flop mode the half cylinder will change its status from engaged to disengaged or vice versa whenever a transponder is operated. This mode is recommendable if, for instance, you want to make a door freely accessible without the use of a transponder.

4. Status reports



Status menu

4.1 Battery condition critical

This checkbox is checked automatically by the programming software when battery capacity starts to decline and status changes to battery warning level 1. Please change the batteries.

4.2 Emergency battery activated

The half cylinder will automatically change to battery warning level 2 if battery capacity continues to decline and the previous warning remains unheeded. The checkbox under item 4.1 is checked automatically by the programming software.
A battery change is now imperative.
The half cylinder automatically changes to emergency battery - warehouse mode after 50 transponder operations or 4 weeks (see chapter 6, Battery warnings).

4.3 Deactivated

This checkbox is automatically checked by the programming software if the half cylinder was deactivated via a SimonsVoss shunt lock or the SimonsVoss network.

4.4 Emergency switch activated

Half cylinders installed within a SimonsVoss network can be permanently engaged automatically via an automated command in the programming software. The signal is usually transmitted by a fire detection system and can be interpreted by the LDB (if configured accordingly).

4.5 Time-controlled opening active

This box is checked if the time-switch function has been programmed and the half cylinder engaged automatically by the time switch.

4.6 Engaged

This box is checked if the time-switch function or flip-flop mode has been programmed and the half cylinder is engaged.

5. Installation instructions

5.1 General notes

When installing the digital half cylinder, make sure no sources of low-frequency radio interference are located nearby. There should be at least 0.5 m distance between individual locking cylinders and 1.5 m between Smart Relays or arming units.

The profile cylinder housing of the half cylinder should not protrude more than 3 mm on the outside. It is also imperative that no water can enter the cylinder through the actuator area.

Do not strike or hit the knob under any circumstances during installation.

The knob is secured by means of a bayonet lock.

Batteries are already installed in the unit on delivery.

The installation work described in this chapter can only be executed with the installation/battery tool.

5.2 Programming the half cylinder

The digital half cylinder and the corresponding transponders must be programmed into the locking plan prior to installation. Please see the software operating instructions for further details.

- Half cylinders are delivered from the factory in so-called warehouse mode; communication with transponders is not possible in this mode (exception: programming transponder). You can deactivate the warehouse mode using the software or programming device without having to create a locking plan. Please see the software operating instructions for further details.

5.3 Installing the half cylinder (except .MR)

Turn the actuator until it is vertical and pointing downwards. Insert the digital half cylinder through the lock. Secure the half cylinder in the slot-in lock with the fixing screw.

- Do not strike or hit the knob under any circumstances during installation.
  The cylinder must not come into contact with oil, paint or acids.

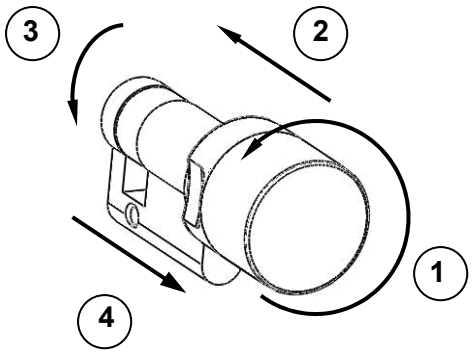
5.3.1 Perform a function test

1. Engage the half cylinder using the transponder; with the door open, turn the knob in both directions for opening and locking. The knob should turn freely in both directions.

2. Close the door and repeat the test. If the knob is difficult to turn, you will need to adjust the door or the striking plate.

The same applies to installation in a key-operated switch.

5.4 Removing the multistage half cylinder



Pease follow these steps if you need to remove the half cylinder:

1. Insert a suitable tool (e.g. a screwdriver) into both grooves of the plastic plate between knob and profile cylinder housing and turn it using gentle pressure. This will destroy the plate.
2. Remove the rest of the plastic plate.
3. Engage the half cylinder using an authorised transponder.
4. When engaged, turn the knob anti-clockwise until it will not turn any further (e.g. up to the lock if it is installed; if it is not installed, hold the actuator with your hand; see illustration step 1).
5. Turn the knob towards the profile cylinder housing until it will not turn any further (audible clicking noise! If necessary, move the knob forwards and backwards a number of times until you hear the clicking sound; see image for steps 2 and 4).
6. If necessary, engage the half cylinder once again using an authorised transponder.
7. Turn the knob anti-clockwise with the half cylinder engaged and hold it against the stop (see image step 3).
8. Hold the knob against the stop and pull it away from the profile cylinder housing together with the inner tube (see image for step 4).

☝ Do not strike or hit the knob under any circumstances during installation. The cylinder must not come into contact with oil, paint or acids.

5.5 Installing the multistage half cylinder

1. Remove the metal plates from the inner tube and slide a plastic plate on to it. (The plastic plates are included in the packaging!)
2. Now slide the metal plates back on to the inner tube so that **one** plastic plate and a number of metal plates determined by the half cylinder model are located on the inner tube.
3. Carefully insert the inner tube into the profile cylinder housing up to the stop.
4. Use an authorised transponder to engage the half cylinder.
5. With the half cylinder engaged, push the knob lightly against the profile cylinder housing whilst turning it clockwise until the inner tube snaps into the profile cylinder housing.

   - Pull lightly on the knob whilst turning to and from to check whether the inner tube has snapped properly into place.
   - The plastic plates are included in the packaging!

When you assemble the unit, make sure that only **one** plastic plate and the exact same number of metal plates as during disassembly are located on the inner tube! The plastic plate must be located directly against the knob.

5.5.1 Perform a function test

1. Engage the half cylinder using the transponder; with the door open, turn the knob in both directions for opening and locking. The knob should turn freely in both directions.

2. Close the door and repeat the test. If the knob is difficult to turn you will need to adjust the door or the striking plate.

The same applies in general to installation in a key-operated switch.

6. Battery warnings

Each half cylinder has a battery management system that indicates declining battery power in good time. This helps prevent the batteries from becoming completely discharged. The battery warning levels are described in the following.

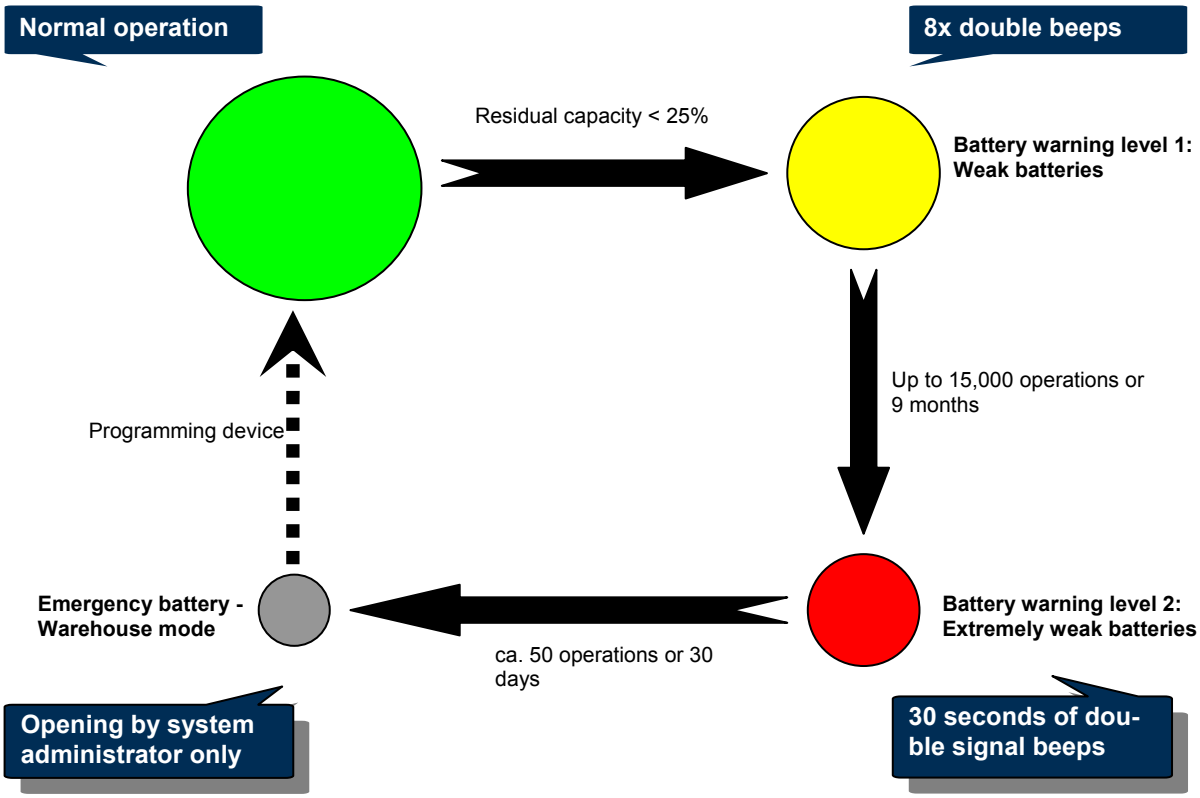
6.1 Half cylinder

Warning level 1: weak batteries
When a half cylinder's batteries are running low it will emit eight short signal tones in rapid succession when operated by a transponder before the cylinder engages. The batteries should be replaced without delay. Around 15,000 opening or 9 months use of the half cylinder remain after battery warning 1 has been triggered.

Warning level 2: extremely weak batteries
If the batteries are allowed to discharge even further, subsequent transponder operation will induce a succession of short signal tones lasting approximately 30 seconds before the cylinder engages. The cylinder will not engage until after the acoustic signal has ended. The batteries are now virtually completely discharged. It is imperative they are replaced as soon as possible.

Emergency battery - warehouse mode:
A half cylinder that has indicated battery warning level 2 will remain active for approximately another 50 operations, or it will shut down completely after approximately 30 days if not used. In both cases the half cylinder will revert back to the so-called emergency battery - warehouse mode. The half cylinder can now only engage with the help of a programming device (see chapter 6.1.3). Batteries can be changed at any time when the half cylinder is in emergency battery - warehouse mode.

6.1.1 Schema



6.1.2 Procedure for emergency battery - warehouse mode

Please proceed as follows to change the batteries if the half cylinder is in emergency battery - warehouse mode:

- Replacing batteries (see chapter Battery change).
- Go to the door and take a Notebook or PDA (having exported the locking plan) and a programming device with you.
- Select the appropriate locking from the locking plan.
- Program over the cylinder once without making any changes. This deactivates the two battery warning checkboxes and the warehouse mode.
- Use the authorised transponder to engage the cylinder.

The half cylinder will emit the level 2 battery warning once more after the batteries have been changed. The locking cylinder's electronic system will then detect that the batteries are at full capacity or have been replaced and the cylinder will work as normal.

This procedure is only necessary in emergency battery - warehouse mode. This mode was introduced to prevent the batteries from completely discharging without intervention by the locking system administrator. Nonetheless, batteries in emergency battery - warehouse mode should be changed as soon as possible.

6.2 Transponder

When the transponder's battery voltage starts to decline, each transponder operation will cause the half cylinder to emit eight short signal tones in rapid succession after it has disengaged.

7. Signal tones

Signal type	Meaning	Required action
2 short tones prior to engaging and one short tone after disengaging	Normal operation	None
Battery warning level 1: 8 short tones prior to engaging	Batteries will soon be empty	Change the cylinder batteries
Battery warning level 2: **8 short tones for 30 seconds with a one-second break between each set**	Batteries are nearly completely discharged	**Replace the cylinder batteries immediately!**
8 short tones after disengaging	Transponder battery empty	Have the transponder battery changed
1 short signal tone without engaging the cylinder	• Attempt to operate outside of time zone • Armed alarm system with simultaneous use of a SimonsVoss shunt lock	None

8. Battery change

8.1 General notes

Batteries should only be changed by trained personnel. Only use batteries approved by SimonsVoss.

Please see the data sheet for further information.

- Reversing polarity can result in damage to the locking cylinder. The batteries used in this device can cause fire or burns if handled incorrectly. Do not charge, open, heat above 100°C, short-circuit or burn batteries.

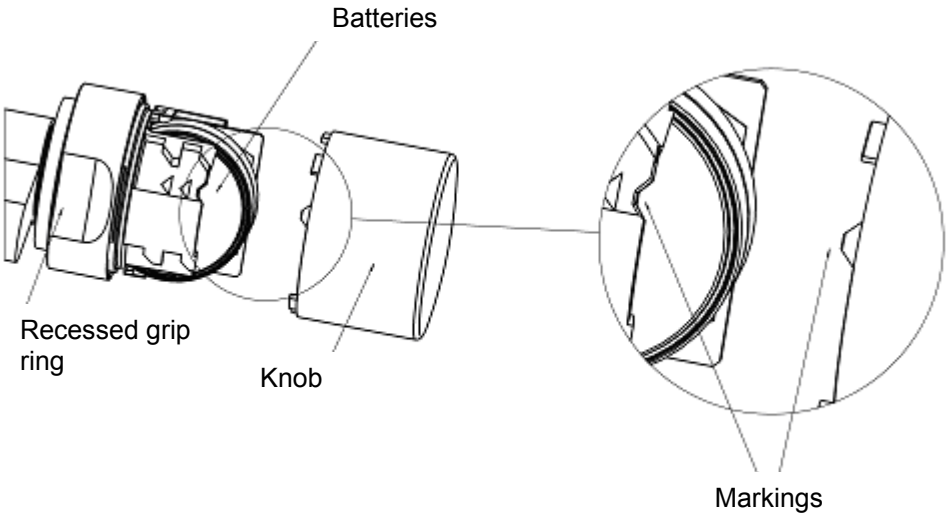
- Please dispose of discharged lithium batteries immediately. Keep out of reach of children. Do not open batteries. Do not throw them into the fire.

Always replace both batteries together at the same time.

Please also see the safety notes in chapter 1.1.

8.2 Procedure

1. Hold the assembly/battery tool against the knob so that both nibs fit into the openings on the ratchet disk (if necessary turn the knob until the nibs slot into the openings).
   Attention: The assembly/battery tool must be held flush against the inner surface of the recessed grip ring to fit into the ratchet disk.
2. Hold the knob and carefully turn the assembly/battery tool 30° in a clockwise direction (until you hear a clicking noise).
3. Remove the assembly/battery tool from the knob.
4. Slide the recessed grip ring back towards the door until it slips off the knob.
5. Hold the recessed grip ring, turn the knob approx. 10° anti-clockwise and remove.
6. Carefully remove both batteries from their bracket.
7. Hold the two new batteries with plus poles facing each other and slide them into the bracket (please replace the batteries as quickly as possible). Make sure you wear clean, grease-free gloves when handling new batteries.



8. Replace the knob (according to the triangular markings, see drawing), hold the recessed grip ring and turn the inner knob (approx. 10°) in a clockwise direction to tighten.
9. Slide the recessed grip ring back onto the knob so that the knob and ring are flush against each other.
10. Hold the assembly/battery tool against the knob so that both nibs fit into the openings on the ratchet disk (if necessary turn the knob until the nibs slot into the openings).
11. Lock the knob by turning it approx. 30° in a clockwise direction (until you hear a clicking noise).

Use an authorised transponder to check functionality.

👍 When replacing the batteries on a ZK version you may have to reset the time as the clock will stop running when the power supply is interrupted (software operating instructions: Programming → Set locking clock time).

9. Possible uses

9.1 General

The digital locking cylinder is designed to fit locks for Euro profile cylinders compliant with DIN 18252 and EN1303.

9.2 Outdoor installation situations

Unless it is ensured that the door is completely water-proof it is recommendable to use the .WP version of each respective model.

9.3 Key-operated switches

The multistage cylinder should be used for key-operated switches in the interest of safe and secure operation.

10. Accessories

10.1 Tool

Assembly/battery tool. The tool is used to change the half cylinder batteries.

10.2 Battery set

A battery pack is available to order. The set contains 10 batteries of type CR2450. Please only use batteries approved by SimonsVoss.

11. Data sheet

Knobs	Material	Stainless steel
	Colours	Satin stainless steel
	Diameter	30 mm
	Length	37 mm (from profile face)
Profile cylinder	Basic length	External 30 mm, internal 10 mm Design lengths in increments of 5 mm (no kits) up to 100 mm overall length, whereby the external side of the cylinder can be up to a maximum of 90 mm in length. Longer lengths are available on request.
Batteries	Type	CR 2450
	Manufacturer	Varta, (Panasonic, Sony)
	Quantity	2 pieces
	Voltage	3 Volt
	Lifetime	approx. 150,000 operations or approx. 6-7 years on stand-by
Ambient conditions	Operating temperature	-20°C to +50°C
	Storage temperature	-30°C to +60°C
	Protection Class	IP 54 (when installed) Variant .WP: IP 65 (knob)

Smart Relay:
SREL, SREL.ZK, SREL.AKV

State of: September 2006

SimonsVoss technologies

Content

1.0 Important Information 4
2.0 Product Description 4
3.0 Before Ordering 5
3.1 Determine Which Version of the Smart Relay you need 5
3.2 Determine Which Accessories you need 5
3.3 Dimension and Procure Power Supplies 5
3.4 Determine the Installation Position 6
3.5 Additional Information: 6
4.0 Before Installation 6
4.1 Installation of the Backup battery 7
5.0 Installation 8
6.0 Connection Assignments 9
6.1 SREL and SREL.ZK 9
6.2 SREL.ADV 10
6.3 Description of the SREL, SREL.ZK and SREL.ADV Connection 10
7.0 Programming and Configuration 11
7.1 Access control 12
7.2 Time zone control 12
7.3 Overlay 12
7.4 Flip Flop 12
7.5 Repeater 12
7.6 Time switching 12
7.7 OMRON 13
7.7.1 The Smart Relay in OMRON Mode 14
7.8 No acoustic programmer acknowledge 15
7.9 External beeper/ External LED 15
7.10 Internal/ external antenna 15

Content

7.11 Number of expansion modules 15
7.12 Pulse length 15
7.13 Interface 16
7.14 Restricted range 16
7.15 External Beeper/ External LED 16
7.16 Log unauthorised accesses 17
8.0 Serial Interface 18
8.1 Functional Description 18
8.2 Wiegand Interface (32 bit and 26 bit) 18
8.3 Kaba Benzing, Siemens, Gantner Legic, Primion, Isgus Interface 19
9.0 Maintenance 19
9.1 Battery Warning and Battery Replacement if you are using the SREL.BAT battery 19
9.2 Backup Battery 20
10.0 Data sheet 21

1.0 Important Information

Safety remark:
Caution! – Incorrect handling of the batteries and storage batteries used in this product can result in the risk of fire or burns. Do not charge, open or burn these batteries or heat them to more than 100 °C (212 °F).

Installation of a SimonsVoss Smart Relay requires knowledge in the areas of door mechanics, door certifications, installation of electronics and the use of the SimonsVoss software. For this reason, only trained and authorised personnel should install the unit.

SimonsVoss Technologies AG will not accept any liability for damages caused by incorrect installation.

Incorrectly installed Smart Relays may block the access through a door. SimonsVoss AG is not liable for the consequences of incorrect installation, such as blocked access to injured or endangered persons, property damage or other damages.

If you will be storing the Smart Relay for more than one week, remove the backup battery.

The Smart Relay must be installed in compliance with ESD (electrostatic discharge) guidelines. In particular, contact with the printed circuit boards and the switching circuits integrated on them must be avoided.

2.0 Product Description

The SimonsVoss Smart Relay is an electronic switch that you can switch with a SimonsVoss transponder. You can use the SimonsVoss software to configure the authorisation for transponders that are permitted to operate the Smart Relay. As a result, the Smart Relay offers the full function of an access control reader.

3.0 Before Ordering

3.1 Determine Which Version of the Smart Relay you need

1. Smart Relay basic version: ordering code SREL

   This relay allows simple yes/no authorisation for up to 8184 different transponders.

2. Smart Relay TZC version with access logging and time zones: ordering code SREL.ZK.

   Like the basic version, but with the capability of separately switching on access logging for the last 1024 accesses (for firmware version 4.0.01.15 and later), with date and time, or day-time zones for up to five groups of people, and automatic locking and unlocking.

3. Smart Relay Advanced version, ordering code SREL.ADV

   Like the TZC version, but with the following additional functions:
   - Connection for external modules using a three-wire bus
   - Connection of an extended antenna
   - Connections for serial interfaces to external time recording terminals or access control readers
   - Connection for external LED or buzzer

3.2 Determine Which Accessories you need

Extended antenna for unfavourable reception conditions ordering code: SREL.AV

Battery only for SREL, SREL.ZK and SREL.ADV in case you will be operating these products without an additional supply voltage: ordering code SREL.BAT

3.3 Dimension and Procure Power Supplies

These power supplies are necessary for all Smart Relays that will not be battery operated. The power supply should have an output of no more than 15 watts and should be capable of delivering voltage of 12 VAC or 5 to 24 VDC when the current is 100 mA.

Attention! Do not user any switched-mode power supplies near the Smart Relays.

The customer must provide all power supplies; they are not available from SimonsVoss.

3.4 Determine the Installation Position

The range from the transponder to the Smart Relay (reader range) is a maximum of 1.5 m (5 feet), but can be dampened by a metal environment (particularly by strong magnetic fields or aluminium).

Ideally, you should conduct a range test with an authorised transponder and a battery-operated Smart Relay.

3.5 Additional Information:

- All cables for connecting to the Smart Relay should be type IY(ST)Y ....x0.6 (Twisted-Pair shielded cable). The maximum cable length should not exceed 100 m (approximately 330 feet). At the same time, you must take into account the power losses when you dimension the supply voltage.

- You must take into consideration the technical specifications for the inputs and outputs (see Technical Data)

- You must lay and connect all cables according to VDE standards.

4.0 Before Installation

- Unpack the Smart Relay and check for any damages.

- Connect the Smart Relay to a supply voltage or battery.

- If you are operating the Smart Relay with a power supply, insert the backup battery included in the delivery into the holder provided for it (see Installation of the Backup Battery).

- Verify the function of the Smart Relay with a transponder in the condition as received from the factory.

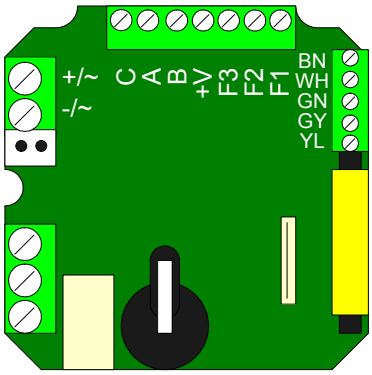
- If you are installing the Smart Relay in a flush socket device, remove the housing.

- If you are installing the Smart Relay on the wall, you can use the bottom plate as a template for the bore holes (6 mm).

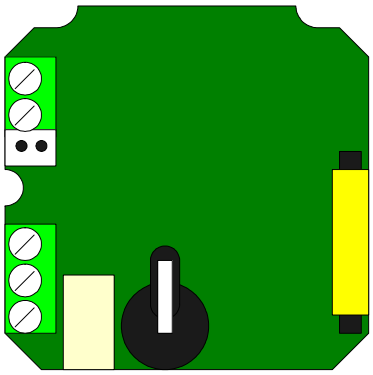
4.1 Installation of the Backup battery

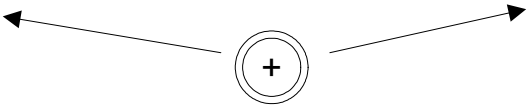
Insert the battery only if you will be operating the Smart Relay with the power supply. Do not insert this battery if you will be operating with the SREL.BAT!

SREL.ADV



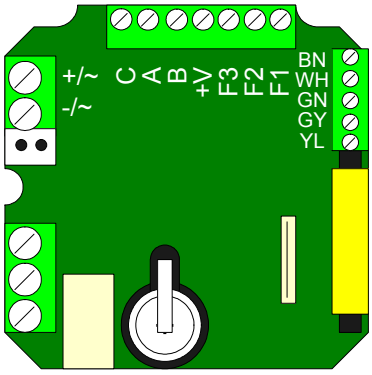
un SREL and SREL.ZK



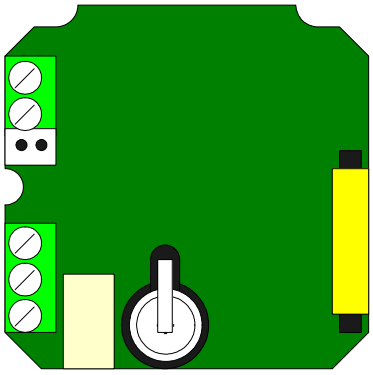


Insert the backup battery (included in the delivery) in the holder
POSITIVE POLE UP

SREL.ADV



un SREL and SREL.ZK



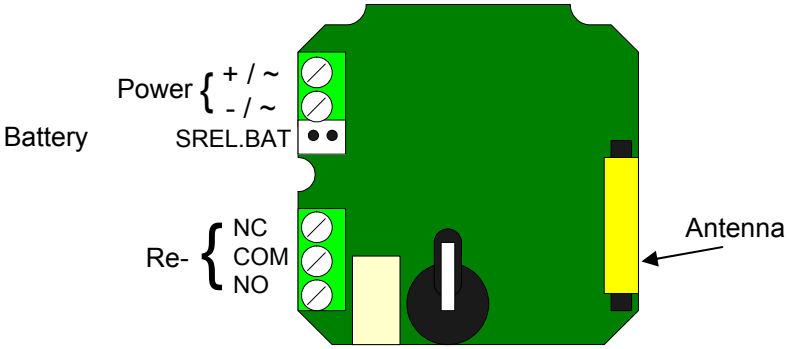
5.0 Installation

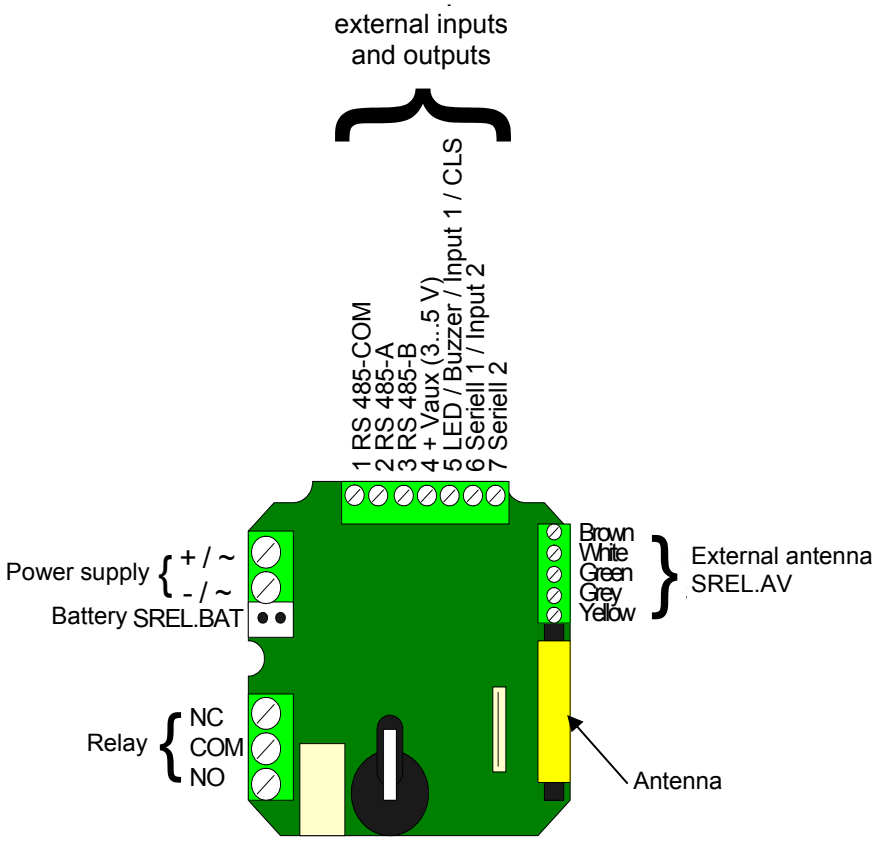
- Switch off the supply voltage (if necessary, pull out the plug or disconnect the battery).
- Connect all cables to the terminals provided on the Smart Relay (see Connection Assignments on the following page)

  If you are connecting a direct current power supply, make sure that you get the polarity right.
- You can attain the largest reader range if you align the Smart Relay antennas so that they are parallel to that on the transponder during the installation.
- Switch on the supply voltage (if necessary, insert the plug or connect the battery).
- Verify the function of the Smart Relay with a transponder in the condition as received from the factory.
- Program the Smart Relay with the SimonsVoss software (we recommend software version LDB.EXE 1.40 or later).
- Use a transponder that is now authorised in order to test the functioning of the Smart Relay again.

6.0 Connection Assignments

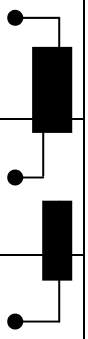
6.1 SREL and SREL.ZK





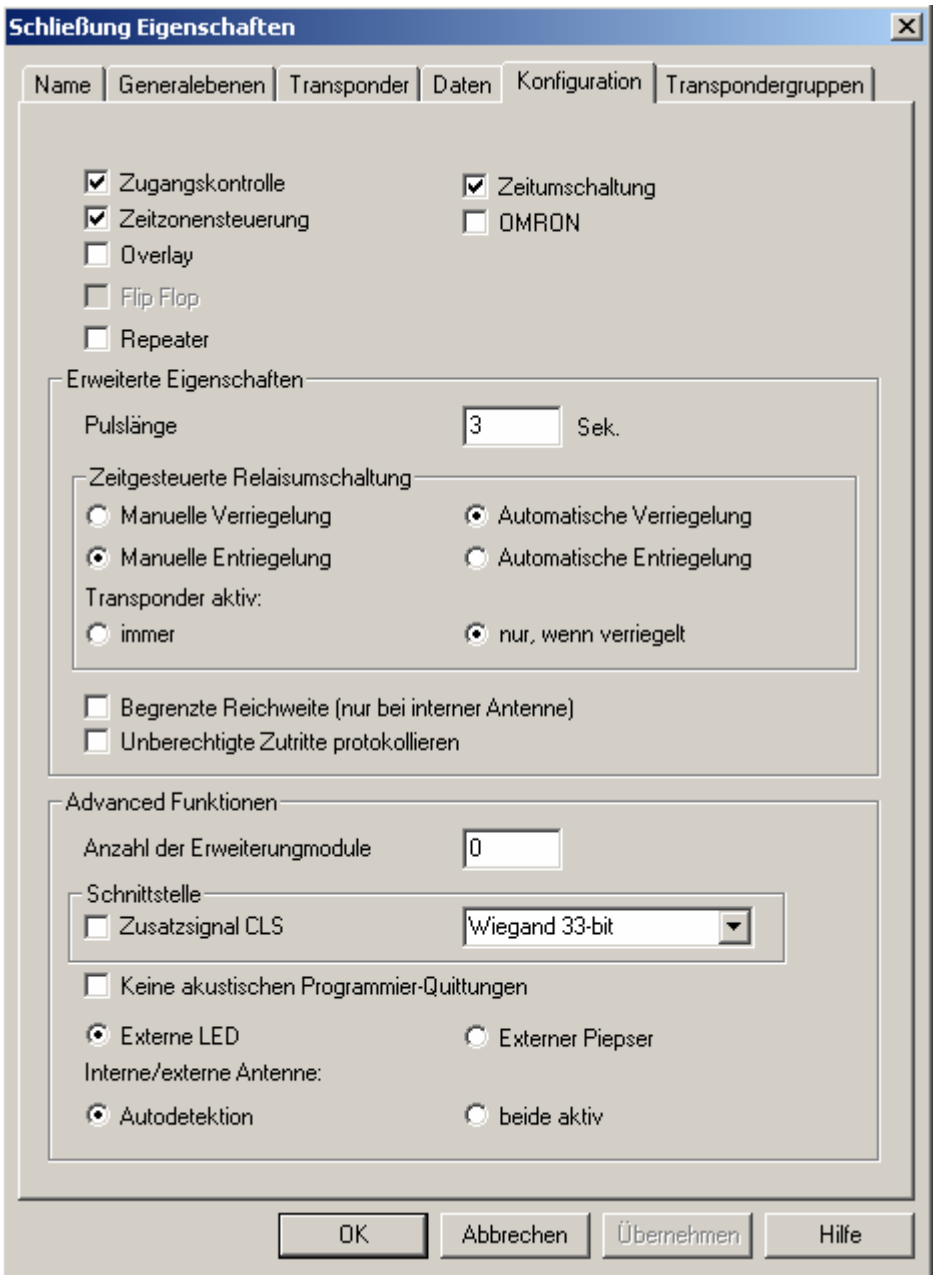
6.2 SREL.ADV

6.3 Description of the SREL, SREL.ZK and SREL.ADV Connection

Name	Symbol	Description
Power supply	+ / ~	If connecting a direct current (5 to 24 VDC) source, use the positive pole, otherwise use one of the two alternating current connections (12 VAC)
Power supply	- / ~	If connecting a direct current (5 to 24 VDC) source, use the negative pole, otherwise use the second alternating current connection (12 VAC)
Battery		Plug connection for a battery (when operating without a power supply) Battery ordering code, incl. connector: SREL.BAT
NC relay 		Normally closed contact for the change-over relay. When not acted on, this contact is closed to the COM relay
COM relay		Common contact on the change-over relay. This contact is either wired to the NC relay (normally closed contact) or to the NO relay (normally open contact)
NO relay		Normally open contact on the change-over relay. When acted on, this contact is closed to the COM relay
External antenna Brown White Green Grey Yellow	 BN WH GN GY YL	Connection for the coloured cables of an extended antenna (ordering code SREL.AV)
RS-485COM RS-485A RS-485B	C A B	Bus connection for external modules
+ Vaux	+V	Typically 3.0 - 5.0V +/- 0.5V for external LED's or buzzer, max. 10mA
LED/ Buzzer/ Input 1/ CLS	F3	Multifunction connection
Serial 1/ input 2	F2	Multifunction connection
Serial 2	F1	Multifunction connection

7.0 Programming and Configuration

When you choose Smart Relay as the locking type in the SimonsVoss software (Version 1.40 and later), you have the following configuration option's:



7.1 Access control

Only possible for SREL.ZK and SREL.ADV
The last 1024 transponder activation's are saved with the date and time.

7.2 Time zone control

Only possible for SREL.ZK and SREL.ADV
You can load a time zone plan and the transponders are then approved or blocked, according to their time zone group.

7.3 Overlay

Replacement transponders can overwrite the transponders that they replace. After the first operation with a replacement transponder, the system blocks the original transponder.

7.4 Flip Flop

Pulse mode (default setting) is switched off, and the pulse width does not matter any more. When flip flop mode is switched on, the Smart Relay changes its state from ON to OFF or back again, each time the transponder is activated. We recommend this mode for switching lights or machines, etc.

With an installation of this kind, it may be necessary to make sure that the power supplies and door openers are suitable for continuous current operation.

7.5 Repeater

The Smart Relay receives a transponder signal and then sends it again, amplified. You can use the Smart Relay in this function in order to link a way through larger radio paths. The distance to another Smart Relay can be up to 2.0 m (6.5 ft).

7.6 Time switching

Only for SREL.ZK and SREL.ADV
If time switching is activated, you must load a time zone plan, which allows a general release of the Smart Relay during the marked times (in Group 5). This means that a door can be freely accessible during the day but only opened by transponder at night.

With an installation of this kind, you must make sure that the power supplies and door openers are suitable for continuous current operation.

If you select time switching, the "Time-controlled relay switching" field has the following option's (you may select more than one):

1. Manual locking:
   The door is not locked automatically according to the selected time of day, but instead only after an authorised transponder is operated after this time.

2. Automatic locking (default setting):
   The door is locked at exactly the time stored in the time zone plan.

3. Manual unlocking (default setting):
   The door is not unlocked automatically according to the selected time of day, but instead only after an authorised transponder is operated after this time.

4. Automatic unlocking:
   Normally, the door is not opened at the selected time of day, but instead only after operation with the first transponder. If it is required that the door always open automatically at the selected time of time, then select this option.

5. Transponder active:

   - Always:
   Normally, a transponder cannot be used during the released periods. If it is necessary, however, to be able to lock the door during this time (for example, if everyone leaves the building), then select this option.

   - Only when locked:
   In this operating mode, the transponder has no effect during the released time.

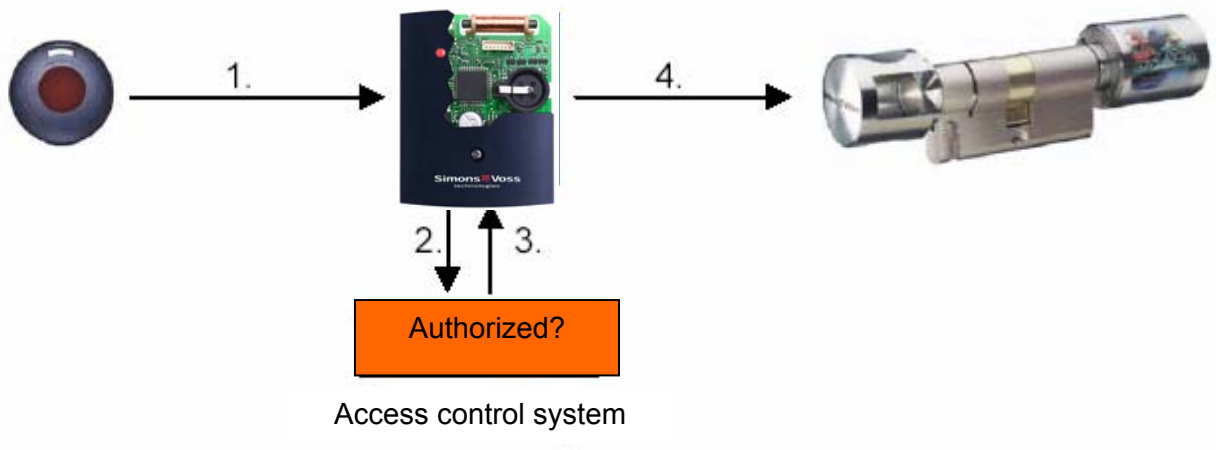
7.7 OMRON

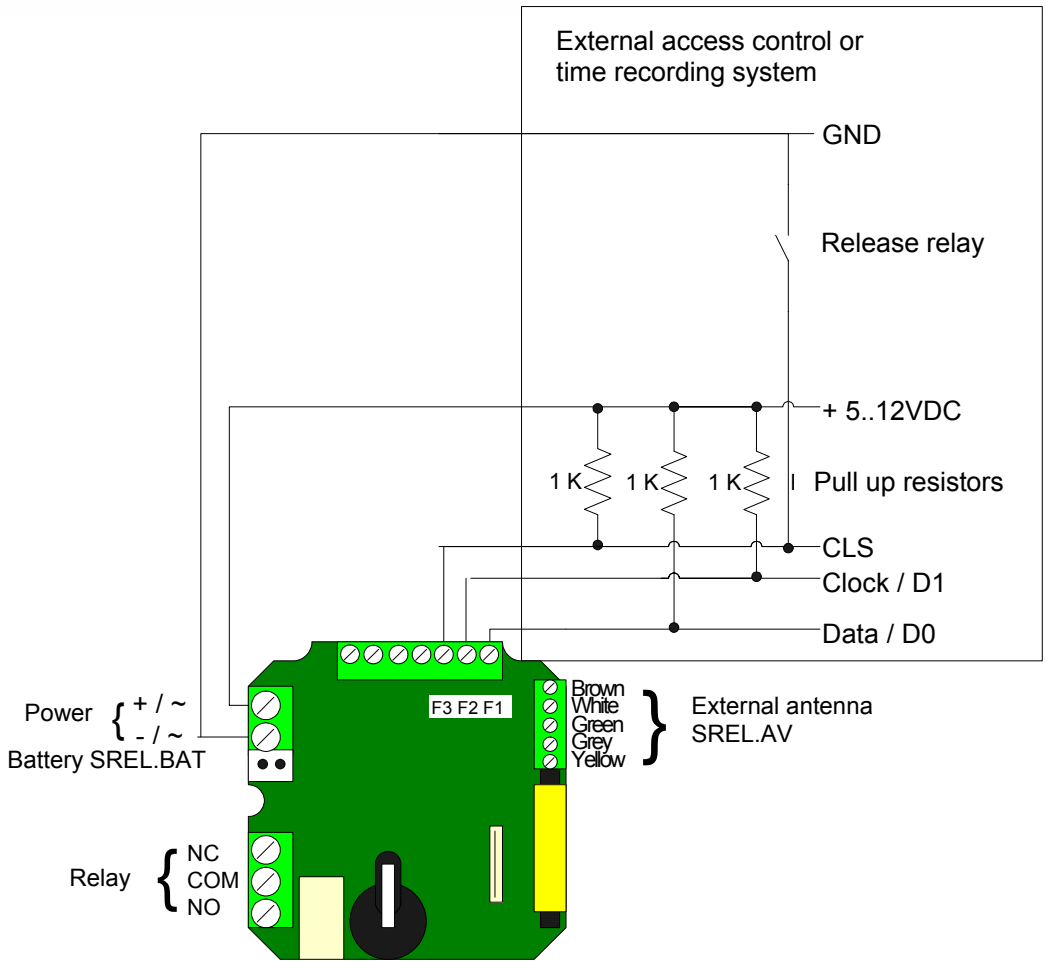
Only for SREL.ADV
Many access control and time recording systems have serial interfaces for connection to card readers. It is also possible to connect a Smart Relay over these interfaces. This means that you can also use the SimonsVoss transponder in systems from other companies.

If you would like the Smart Relay to transmit the transponder data to such an external system, and for the Smart Relay to send a remote opening command to a cylinder when released by this external system, then select this option, both on the Smart Relay and on the cylinder.

Select the type of external system under "Interface" (7.13). The following types are available:

7.7.1 The Smart Relay in OMRON Mode





7.8 No acoustic programmer acknowledge

Only SREL.ADV
Mark this field if you want no programmer acknowledge to be given via a connected buzzer/beeper when the Smart Relay is programmed.

7.9 External beeper/ External LED

Only SREL.ADV
This is where you specify which external unit is connected. In Flip Flop mode, the Smart Relay generates a continuous signal when switched if there is an external LED connected; if a beeper is connected, it briefly acknowledges each change of state with a sound signal.

7.10 Internal/ external antenna

Only SREL.ADV

- Autodetection:
  If an external antenna is connected, only this antenna is used. The Smart Relay then switches the internal antenna off. If no external antenna is connected (default case), the Smart Relay works with the internal antenna.

- Both active:
  The Smart Relay can assess entries from transponders at both antennas.

7.11 Number of expansion modules

Only for SREL.ADV
This is where you indicate the number of external modules that are connected to the Smart Relay. These modules are connected to terminals RS-485 **C**OM, RS-485 **A** and RS-485 **B**. For more information, refer to the documentation for the separate modules.

7.12 Pulse length

This is where you specify the value, in seconds, for the pulse width of the switching pulse. The value has a range from 0.1 to 25.5 seconds. For example, if you enter 3 seconds here, then a door opener will be released for 3 seconds before it is then blocked again.

7.13 Interface

Only for SREL.ADV
For operation as a serial interface, you can select the type of card reader here that the Smart Relay should simulate. You have the following option's:

- Wiegand 32 bit
- Wiegand 26 bit
- Primion
- Siemens
- Kaba Benzing
- Gantner Legic
- Isgus

You will find the corresponding cabling information in the chapter "The Smart Relay as a Serial Interface".

7.14 Restricted range

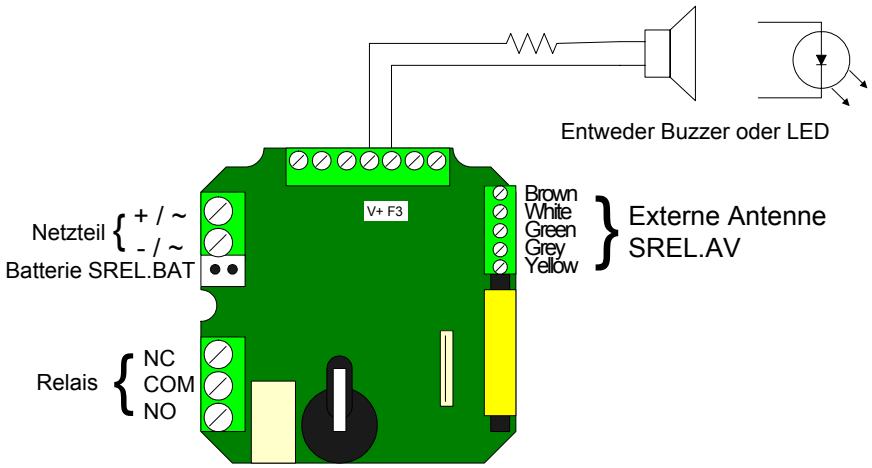
If you select this option, the reader range from the transponder → Smart Relay is restricted from approximately 1.5 m (4.9 ft) down to 0.4 m (1.3 ft). For example, you can use this option if there are several Smart Relays close to one another and individual transponders are authorised for several Smart Relays.

7.15 External Beeper/ External LED

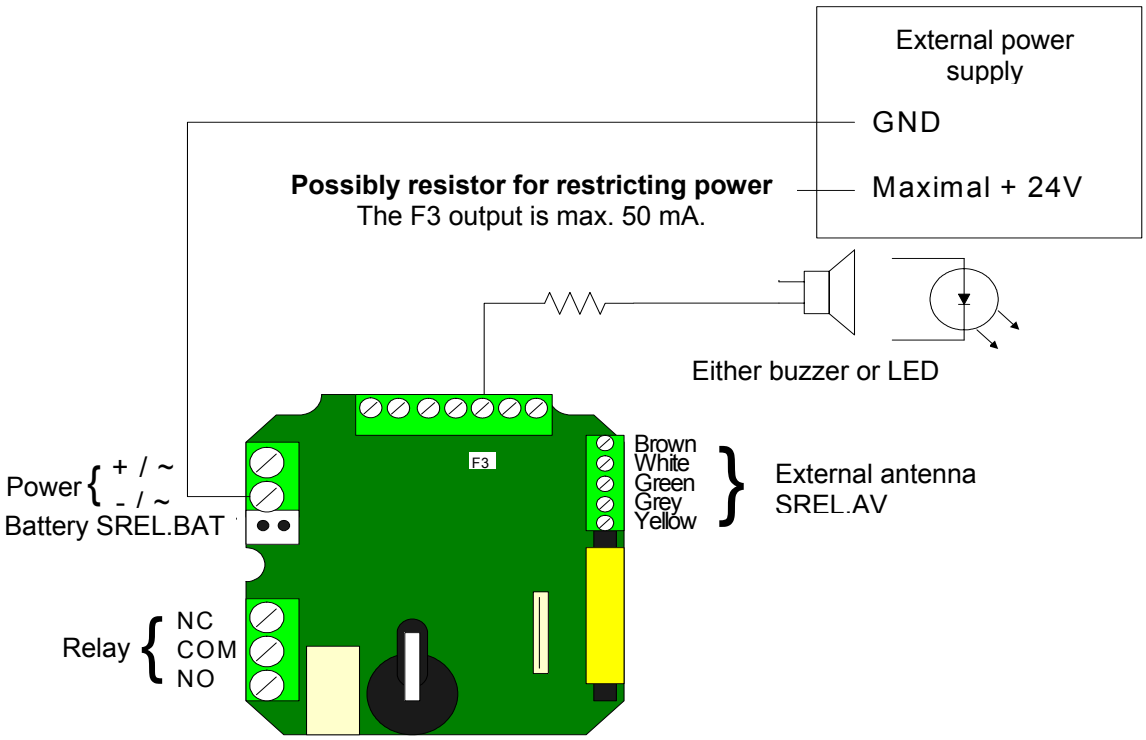
Only for SREL.ADV
Normally, the Smart Relay is configured for connection to an LED. If you want to connect a beeper or buzzer as the external signaller, mark this option. In this way, the beeper/buzzer can be used for an acoustic acknowledgement, instead of the LED.

Should the connected component need less than 10 m maximum current at 3 VDC, the connecting plan can look as follows:

Possibly resistor for restricting power
The V+ output supplies a max. 10 mA at 3 VDC



If the current for the external component is larger than 10 mA, then this component must be fed by an external power supply. In this case, the connection should be made as follows:



7.16 Log unauthorised accesses

Only for SREL.ZK and SREL.ADV
Normally, only authorised transponder operations are logged. If you also want to record attempts to open the door with an unauthorised transponder, you must select this option.

8.0 Serial Interface

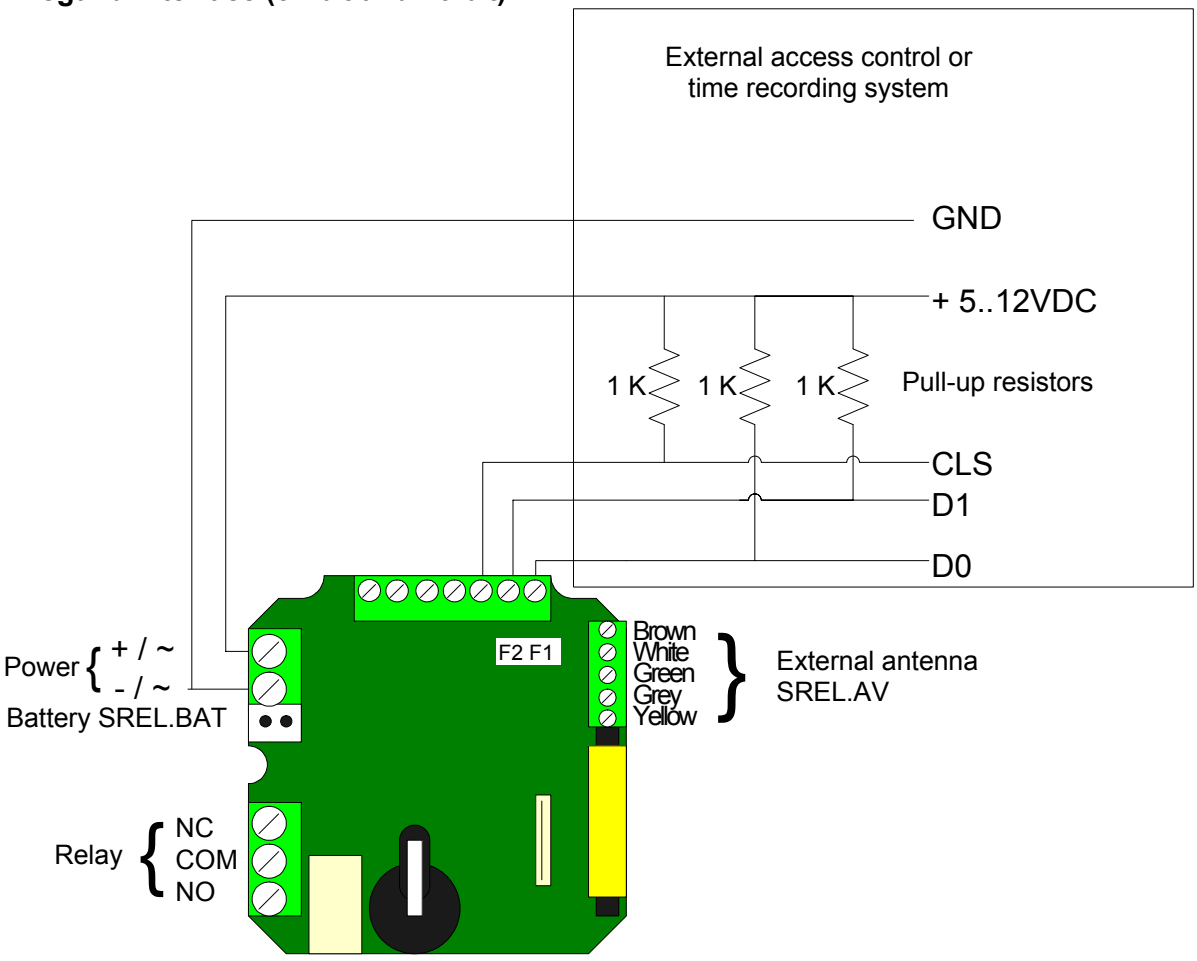
8.1 Functional Description

In order to use a Smart Relay as a card reader in an external access control or time recording system, both the hardware (cable and signal level) and the data formats must correspond exactly to those of the card reader. Only then can the external system understand and evaluate the data from the SimonsVoss transponders.

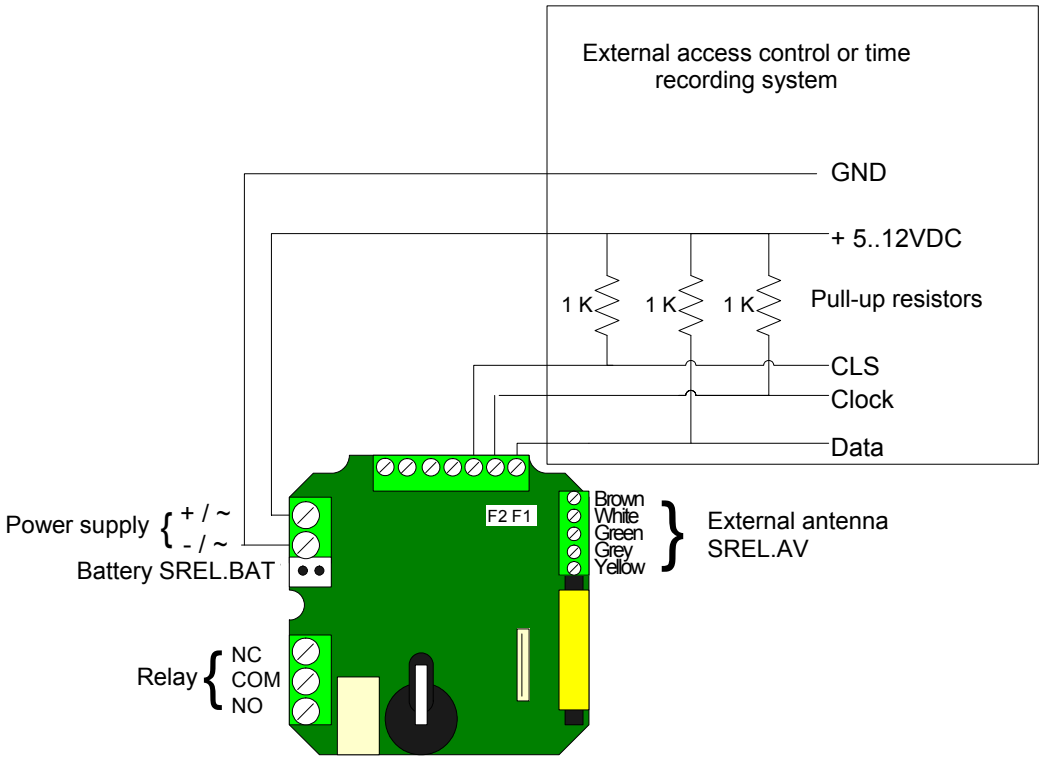
First the Smart Relay reads the transponder data. If the transponder is authorised in the Smart Relay, this data is forwarded to the external system via the serial interface. SimonsVoss Product Management will provide you with detailed specifications for the individual data formats.

You can select the correct reader type in the Smart Relay configuration using the SimonsVoss software, version 1.40 and later. The following sections describe the connections for the different reader versions.

8.2 Wiegand Interface (32 bit and 26 bit)



8.3 Kaba Benzing, Siemens, Gantner Legic, Primion, Isgus Interface



9.0 Maintenance

9.1 Battery Warning and Battery Replacement if you are using the SREL.BAT battery

In case the battery capacity is no longer sufficient, a Smart Relay can issue a battery warning as follows:

SREL, SREL.ZK, SREL.ADV

- Internal LED blinks 8 times each time you operate the transponder and before the relay is switched.

  If you are operating with a battery, you should make sure that this LED can be seen from the outside.

Only SREL.ADV

- External LED blinks 8 times or external buzzer beeps 8 times, each time you operate the transponder.

Approximately 100 operations are possible after the battery warning, so you should replace the battery as soon as possible.

9.2 Backup Battery

A discharged backup battery can cause the internal clock in the type SREL.ZK or SREL.ADV Smart Relay to stop. For this reason, we recommend that you check the time of day at routine intervals. A backup battery will last approximately 10 years if there is no power supply interruption. If the Smart Relay needs the backup battery often because of frequent power failures, you should replace this battery routinely.

If you operate the Smart Relay with a battery (SREL.BAT), you are not permitted to use the backup battery.

10.0 Data sheet

Housing made of black plastic: Dimensions [LxWxH]	72 x 57 x 25.5 mm (approximately 2.8 x 2.2 x 1.0 inches)
Degree of protection	IP 20, not tested for outside use
Temperature	Operation at: -22°C to +55°C (-31°F to +131°F) Storage at: 0°C to +40°C (32°F to +104°F)
Air humidity	<95% without moisture condensation
Printed circuit board dimensions [LxWxH]	50 x 50 x 14 mm (approximately 2.0 x 2.0 x 0.6 inches)
Line voltage	12 VAC or 5-24 VDC (no reverse voltage protection)
Power limit	Power supply must be limited to 15 VA
Quiescent current	< 5 mA
Max. current	< 100 mA
Programmable pulse width	0.1 to 25.5 seconds
Output relay type	Change-over
Output relay continuous current	Max. 1.0 A
Output relay switch on current	Max. 2.0 A
Output relay switching voltage	Max. 24 V
Output relay switching capacity	10^6 operations at 30 VA
Multifunction connections: F1, F2, F3	Max. 24 VDC, max. 50mA
Vibrations	15G for 11 ms, 6 shocks according to IEC 68-2-27 Not released for continuous used under vibrations

Smart Output Module

State of: June 2006

SimonsVoss technologies

Smart Output Module

Content

1.0 Important Information ____ 4
2.0 Product Description ____ 4
3.0 Before Ordering ____ 5
3.1 Smart Relay ____ 5
3.2 Determine the Number of Modules that are Needed ____ 5
3.3 Obtain and Dimension the Power Supply ____ 5
3.4 Determine the Installation Technique and the Installation Site ____ 5
3.5 Cable Types and Paths ____ 5
3.6 Outside Installation ____ 5
3.7 Guidelines ____ 5
4.0 Before Installation ____ 6
5.0 Installation ____ 6
6.0 Connections ____ 7
6.1 Terminal Assignments ____ 7
6.2 Connection Assignments ____ 8
7.0 Connection to the Smart Relay ____ 9
7.1 Standard Power Supply Connection ____ 10
7.2 Emergency Release Connection for a Fire Alarm System ____ 10
7.3 Protective Circuit to Prevent an Opening when the Supply Voltage Fails ____ 11
7.4 Protective Circuit for the Signaling Option Outputs ____ 12
8.0 Programming and Configuration ____ 13
8.1 General Information ____ 13
8.2 Enter the Number of Modules ____ 13
8.3 Select the Module Addresses ____ 13
8.4 Adjust the Pulse Length ____ 14
8.5 Select Signaling ____ 14
8.6 Automatic Name Assignment in the Software ____ 14
8.7 Inverting the Outputs ____ 14

Content

9.0 Meaning of the LEDs _____ 15
9.1 LEDs for Each Output _____ 15
9.2 State LED _____ 15
10.0 Technical Specifications _____ 16

1.0 Important Information

- Installation of a SimonsVoss Smart Output Module requires knowledge in the areas of approvals for electronic and electrical installation and in the use of SimonsVoss software and the SimonsVoss System 3060. For this reason, only trained and expert personnel should install the unit.

SimonsVoss Technologies AG will not accept any liability for damages caused by incorrect installation.

- Incorrectly installed Smart Output Modules may block an entrance or opening. SimonsVoss AG is not liable for the consequences of incorrect installation, such as blocked access to injured or endangered persons, property damage or other damages.

- Should products from other manufacturers be driven with a Smart Output Module, the guarantee and installation conditions given by the respective manufacturer of these devices must be observed.

- Should the maximum permissible currents (see Technical Data) be exceeded at the outputs or should the maximum voltages be exceeded at the inputs of the Smart Output Module, the result can be damage to the module.

2.0 Product Description

The Smart Output Module is a product that provides eight floating relay outputs, which can be driven via a single Smart Relay, type SREL.ADV. Depending on the transponder ID, one or more outputs can be switched for some programmable time. This assignment (profile) can be selected as needed. This means that the Smart Output Module is suitable, for example, for implementing an authorisation-dependent elevator controller or a driver for opening lockers. Should more than eight outputs be required, up to 16 modules can be connected to one type SREL.ADV Smart Relay.

3.0 Before Ordering

3.1 Smart Relay

At least one type SREL.ADV Smart Relay is necessary for operating a Smart Output Module. Please read the Smart Relay Product Manual for information on ordering.

3.2 Determine the Number of Modules that are Needed

Up to 16 external modules can be connected to one type SREL.ADV Smart Relay. If you select the "Signalling" option in the configuration, the number of outputs per Smart Output Module is reduced from eight to four. Each module has a separate configuration in the software.

3.3 Obtain and Dimension the Power Supply

The type SREL.ADV Smart Relay and up to eight type SOM8 external modules can be operated with one power supply (SREL.NT). For the data regarding the power supplies, take the technical specifications (currents, voltages and powers) of the Smart Relay and the modules into consideration.

3.4 Determine the Installation Technique and the Installation Site

The modules are attached to DIN rails. The length of these DIN rails depends on the number of modules that have to be attached next to one another. The Smart Relay Advanced units are typically not mounted on DIN rails, but instead are installed at the place where the transponders should be read.

3.5 Cable Types and Paths

There should be enough room around a Smart Output Module to allow all cables to be laid without kinking them too much. We recommend cable type IY(ST)Y (Twisted-Pair, shielded cable), strand diameter 0.6 mm.

3.6 Outside Installation

A suitable IP 65 (SOM.IP65G) housing must be provided for outside installation.

3.7 Guidelines

The installation should be performed according to VDE guidelines, by experts who have been

4.0 Before Installation

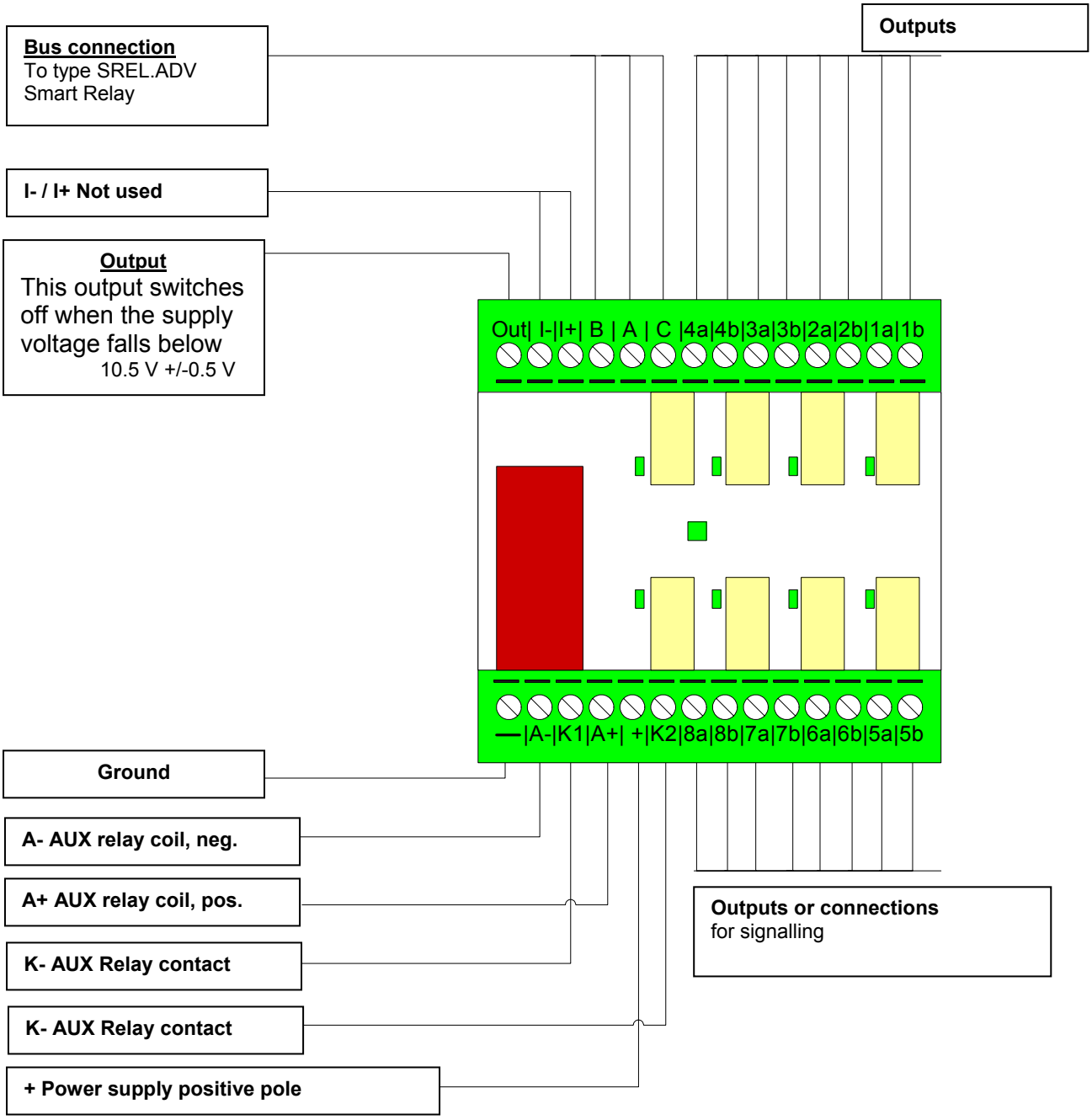
- Unpack the Smart Output Module and inspect it for external damages.
- Connect the Smart Output Module to a type SREL.ADV Smart Relay (see Connection to the Smart Relay) and provide both units with voltage over the power supply.
- Note the polarity.
- Activate the Smart Relay with a transponder in the condition as received from the factory. This activates all Smart Output Module outputs, which is shown by all LED's on the Smart Output Module lighting (green).

5.0 Installation

- Cut the DIN rails to size and tighten the screws.
- Switch off the supply voltage.
- Mount the units on the DIN rail (latch).
- Connect all cables (see Terminal Assignments and Connection Examples).
- Be sure to pay attention to the polarity when connecting the supply voltage.
- Switch on the supply voltage.
- Program the Smart Relay and the Smart Output Module with the SimonsVoss software (see Programming and Configuration).
- Then test the function with authorised transponders.

6.0 Connections

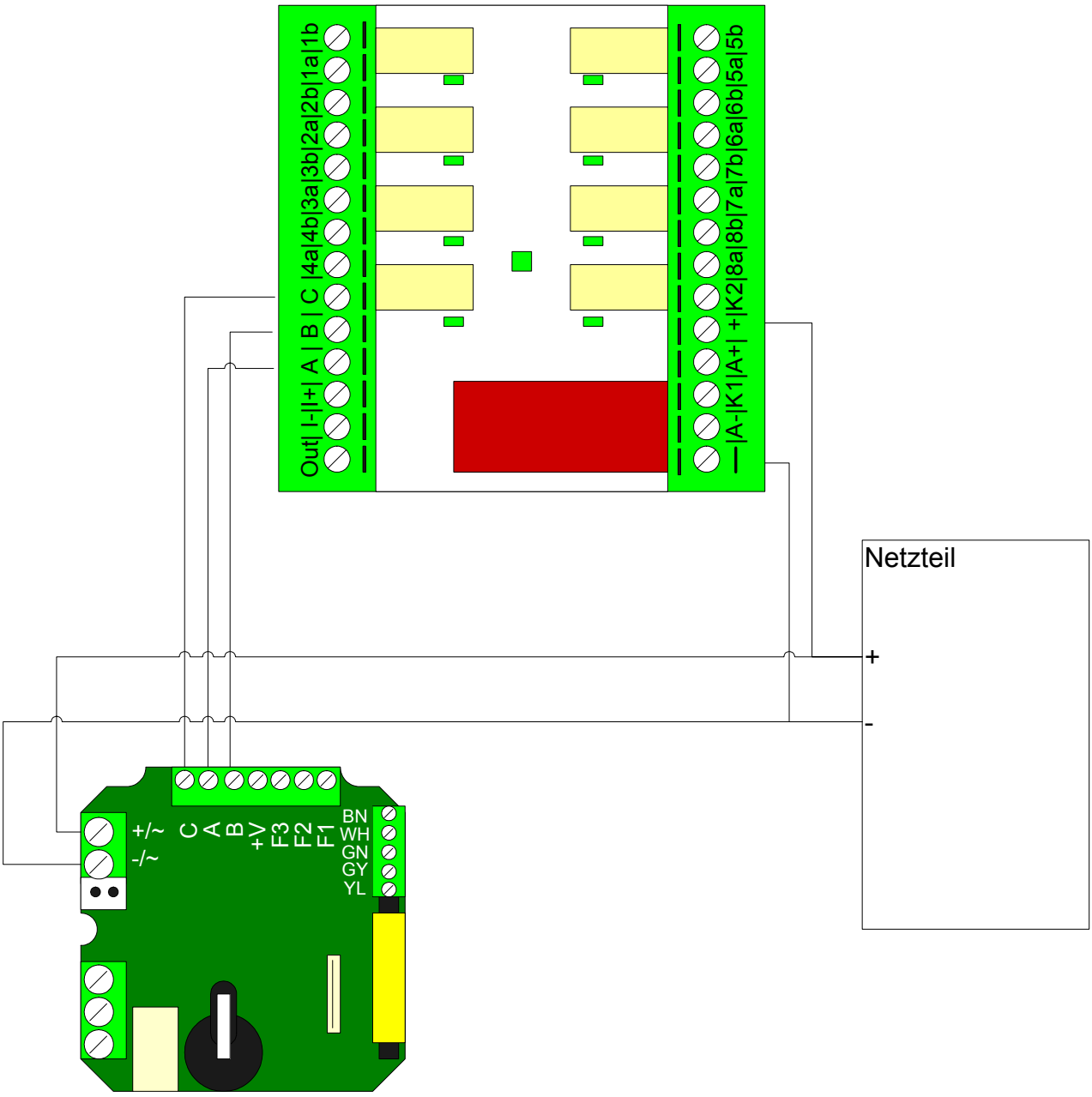
6.1 Terminal Assignments



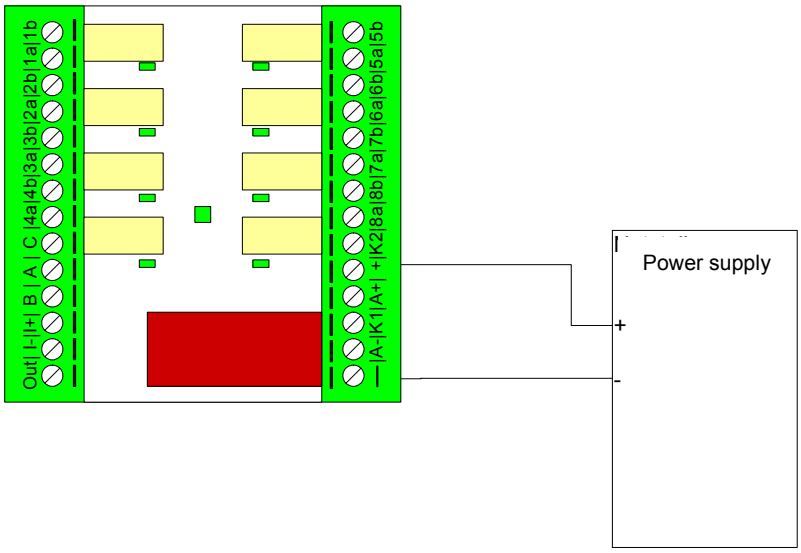
6.2 Connection Assignments

Name	Symbol	Description
Output	Out	If the supply voltage falls below 10.0 VDC +/- 0.5V, this output switches off. Typically, this output is connected to A-, if it is necessary to switch the AUX relay before the switching functions fail. This is an open collector output.
Isolated digital input	I- I+	Not used at this time
Bus connection to the type SREL.ADV Smart Relay	A B C	These terminals are connected to the terminals with the same names on the type SREL.ADV Smart Relay.
Outputs	1a 1b 2a 2b 3a 3b 4a 4b	Floating outputs (make contacts) that are switched depending on the transponder authorisation.
Outputs or connections for signalling	5a 5b 6a 6b 7a 7b 8a 8b	Depending on the configuration Either: floating outputs (make contacts), that are switched depending on the transponder authorisation. Or: floating connections that generate an alternating signal when the assigned output is activated. Assignment: 1 → 5 2 → 6 3 → 7 4 → 8
Name	Symbol	Description
Ground	⏚	Connection for the power supply ground
Plus	+	Connection for +12 VDC
AUX relay coil	A- A+	To switch the AUX relay, this coil must be supplied with 12 VDC.
AUX relay contacts	K1 K2	Floating outputs (make contacts) of the AUX relay.

7.0 Connection to the Smart Relay

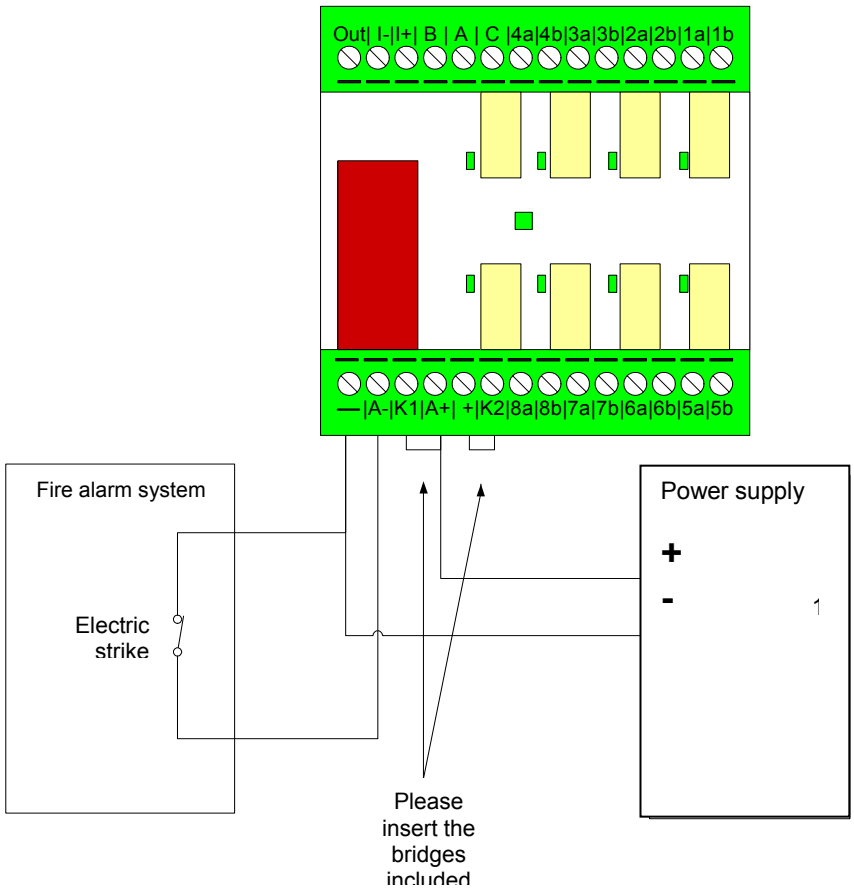


7.1 Standard Power Supply Connection



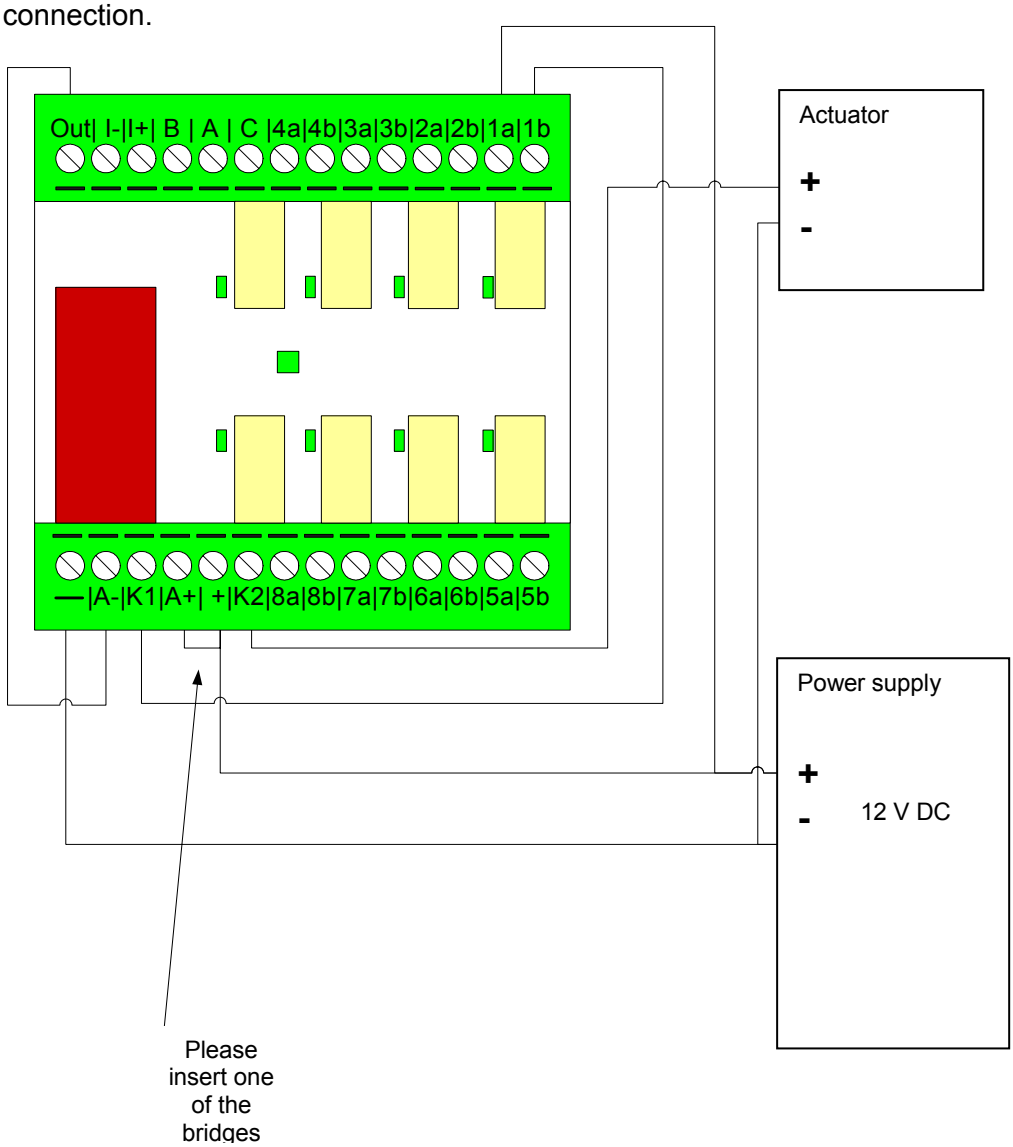
7.2 Emergency Release Connection for a Fire Alarm System

When the fire alarm system relay opens, the Smart Output Module supply voltage is stopped, consequently closing outputs 1 to 8.



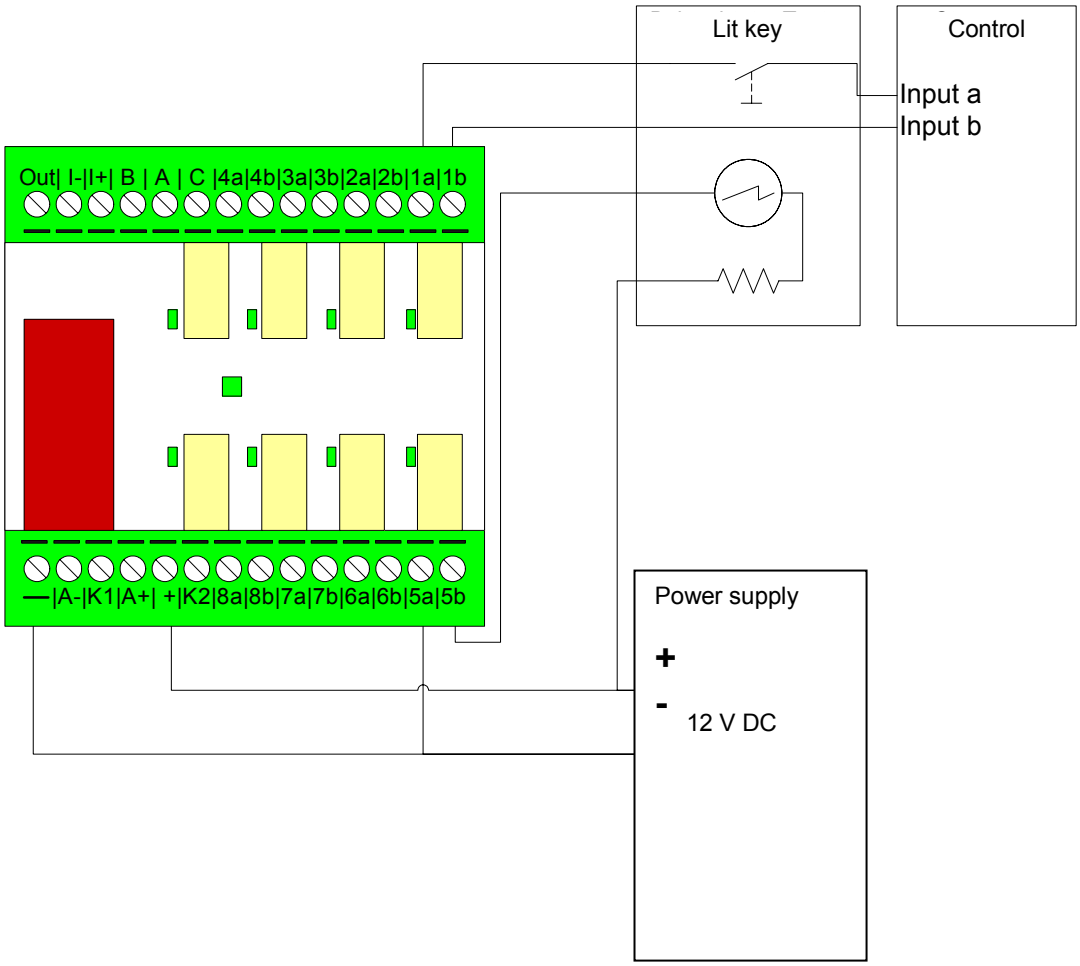
7.3 Protective Circuit to Prevent an Opening when the Supply Voltage Fails

When the supply voltage range falls below the acceptable level, the actuator supply over the AUX relay is interrupted. The switching output (OUT) is used in this connection.



7.4 Protective Circuit for the Signaling Option Outputs

Each pair of terminals opposite one another (1 and 5, 2 and 6, 3 and 7, 4 and 8) works together. When the lower output in the module is switched, the corresponding assigned output blinks.



8.0 Programming and Configuration

8.1 General Information

To program the Smart Output Module, connect it to a type SREL.ADV Smart Relay. Supply power to both the Smart Relay and the Smart Output Module and hold the programming device close to the Smart Relay. The Smart Output Module itself cannot communicate with the Config Device.

8.2 Enter the Number of Modules

Enter the number of connected Smart Output Modules in the Smart Relay configuration. The largest possible value here is 16 modules. This automatically creates lockings in the locking plan for each of a module's outputs.

8.3 Select the Module Addresses

The Smart Relay communicates with each connected module over its address. This address is set up in the Smart Output module using the address switches. The following addresses are permitted:

Modul	**Adresse**
Module 1	0 (default factory setting)
Module 2	1
Module 3	2
Module 4	3
Module 5	4
Module 6	5
Module 7	6
Module 8	7
Module 9	8
Module 10	9
Module 11	A
Module 12	B
Module 13	C
Module 14	D
Module 15	E
Module 16	F

8.4 Adjust the Pulse Length

The modules appear in the locking plan as the locking type "expansion module". You can select a pulse length from 0.1 to 25.5 seconds in the configuration for each module. This length then applies to all of the module's outputs.

8.5 Select Signaling

Signaling is a special function where two of a module's outputs always work together. The first output reacts completely normally, depending on transponder operation; the output assigned to it simultaneously generates an alternating signal. You can select this option, for example, if you want to have the keys that are released when an elevator is controlled blink.

Attention: If you select this option, the number of outputs that are switched when authorized is reduced from eight to four.

Output assignments for signaling:

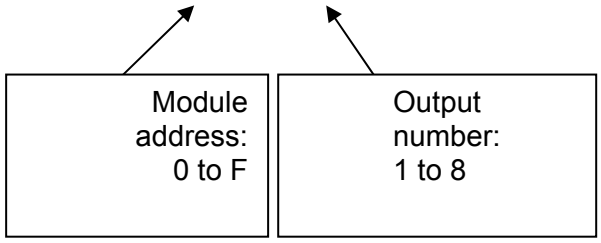
1 → 5
2 → 6
3 → 7
4 → 8

8.6 Automatic Name Assignment in the Software

The SimonsVoss software automatically assigns designation to modules when the modules are created. The following convention is used:

SMART RELAY NAME - MOD0 - OUT1

(z.B. Aufzug1-MOD0-OUT4)



8.7 Inverting the Outputs

This option allows the output switching behavior to be inverted. If there is no supply voltage, all output relays are always closed.

9.0 Meaning of the LEDs

9.1 LEDs for Each Output

Each of the 8 outputs has an LED assigned to it. This LED displays the state of the output.

Green -> output closed
Off -> output open

9.2 State LED

In addition, there is a three-color LED that displays the state of the Smart Output Module:

- **Lights green every 5 seconds** → Communication with the Smart Relay is OK
- **Lights red every 5 seconds** → Communication with the Smart Relay is disrupted. (For example, the bus line has been seized for communication with other modules.
- **Blinks green/red** → Communication currently taking place with the Smart Relay.
- **Blinks red** → The supply voltage is too low.

10.0 Technical Specifications

Housing made of plastic with transparent cover for mounting on DIN rail.	Dimensions: L x W x H 75 x 75 x 53 mm (approx. 3.0 x 3.0 x 2.1 inches)
Weight	Approx. 170 g (approx. 6 ounces) (without packaging)
Degree of protection	IP 20 (not tested for outside use)
Ambient temperature	Operation: 0 – 60°C (32 – 140° F) Storage: 0 – 70°C (32 – 158° F)
Air humidity	<90% without moisture condensation
Supply voltage	11.0 to 15.0 VDC Recommended: 12 VDC regulated
Power limit	The power supply must be limited to a maximum of 15 VA
Quiescent current	<120 mA
Max. current	<150 mA
Programmable pulse width	0.1 to 25.5 seconds
Output relay type	Normally closed
Output relay and AUX relay continuous current	Max 1 A
Output relay and AUX relay switch-on current	Max 2 A
Output relay and AUX relay switching voltage	Max. 24 V
Output relay and AUX relay switching capacity	10^6 operations at 24 VA
Vibrations	15 G for 11 ms, 6 shocks to IEC 68-2-27, not tested for continuous use under vibrations
Output 1 switching current	Max .1 A
Output 1 switching voltage	Max. 24 V
Output 1 switching capacity	Max. 1 VA
Output 1 switching behavior when voltage is too low	V < 10.5 +/- 0.5 V corresponds to off

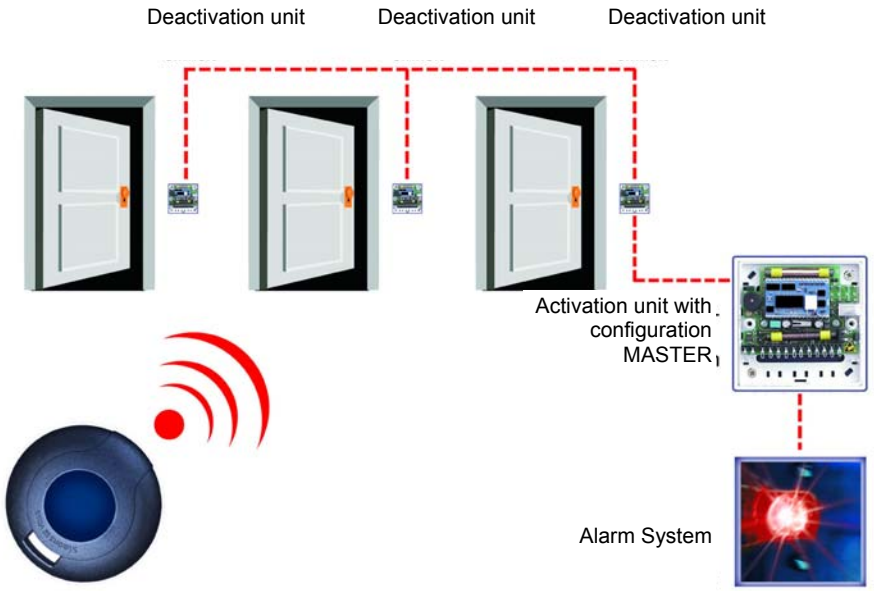
VdS Shunt lock function 3066

Version: September 2006

SimonsVoss technologies

VdS Shunt lock function 3066

Content



1.0 Functional Description ____ 4
1.1 General Information ____ 4
1.2 Safety Remarks ____ 6
2.0 Assembly Instructions ____ 7
2.1 General Information on Installing the Components ____ 7
2.2 Installing the Deactivation Unit (DA) ____ 8
2.2.1 Testing the Deactivation Unit (DA) ____ 9
2.2.2 Connecting Power Supply, Lock Contact Evaluation and Sabotage Contacts: ____ 9
2.2.3 Connecting Deactivation Request and eactivation Acknowledgement ____ 10
2.3 Installing the Master Activation Unit (MA) ____ 11
2.3.1 Testing the Master Activation Unit (MA) ____ 12
2.3.2 Connecting Power Supply, Switch Contacts and abotage Contacts: ____ 12
2.3.3 Connecting Deactivation Request, Deactivation Acknowledgement and Activation Request ____ 13

Content

2.4 Installing the Slave Activation Unit (SA) 14
2.4.1 Testing the Slave Activation Unit (SA) 15
2.4.2 Connecting Power Supply, Sabotage Contacts and Local Activation Suppression: 15
2.4.3 Connecting Deactivation Acknowledgement and Activation Request 16
2.5 Wiring the Shunt Lock Components 16
2.6 Functional Principles 17
3.0 Programming 20
3.1 Programming the Activation Units (MA and SA) 20
3.2 Programming the Deactivation Units (DA) 22
4.0 Installation 24
4.1 Installing the Deactivation Unit 24
4.2 Installing the Activation Unit (MA and SA) 25
4.3 VdS-Compliant Installation of the Activation Unit (MA and SA) 26
5.0 Special Versions of the Shunt lock function 3066 28
5.1 Operating the Activation Unit Without a Deactivation Unit 28
5.2 Operating the Deactivation Unit wthout an Activation Unit 28
6.0 Data Sheet 29

1.0 Functional Description

1.1 General Information

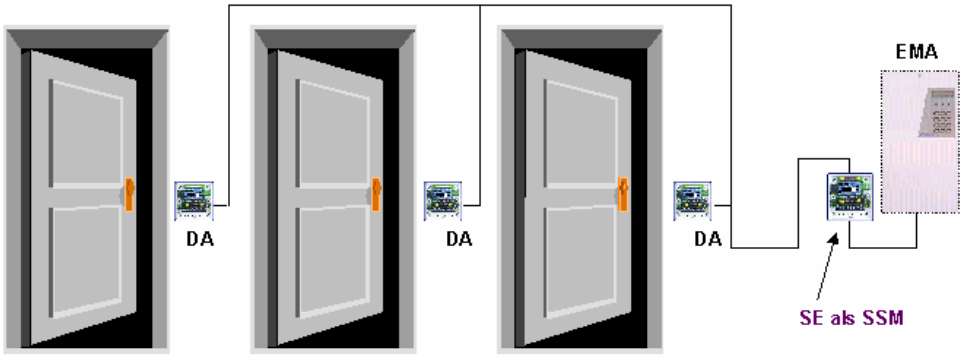
In objects protected by the alarm, measures must be taken to prevent any unintentional entry of the secured area when the alarm system (burglar alarm system, BAS) is activated externally, because this would trigger a false alarm. The Shunt Lock function 3066 implements such a feature without requiring extensive work on the door or doorframe.

The following components are needed for this:

1. Activation unit(s) (MA and SA)
   Such a unit is used to switch the alarm system. You need at least one activation unit (AU) to activate and deactivate the system externally. If you want to be able to activate/deactivate from several locations, you need the corresponding number of activation units. You can use a mouse click to issue the authorizations for activating and deactivating the alarm system in the locking plan.

Basically, there is a difference between the master activation unit (MA) and the slave activation units (SA). The SAs are needed only if you want to activate or deactivate from more than one location. It is always the MA that activates or deactivates the alarm system externally using a floating contact. SAs only send the appropriate requests to the MA. You can also activate internally by using SAs that are separately connected to the internal activation connection of the burglar alarm center (BAC).

2. Deactivation units (DA)
   These are installed next to the doors of the secured area (and in the immediate vicinity of the digital cylinder). They see to it that these doors cannot be accidentally opened even with an authorized transponder if the alarm system has been activated externally. This reliably prevents false alarms.



Switching on the alarm system (burglar alarm system, BAS)

The person with switching authorization presses his or her transponder near an activation unit two times in quick succession (within 2 sec.). This sends a signal to all deactivation units present. If lock contacts are connected to the deactivation units, the DAs first verifies that the doors have been correctly locked. The digital locking cylinders or Smart Relays are not deactivated unless this is the case, so that it is no longer possible to enter the secured area. The activation unit does not receive a positive acknowledgement until all lockings have been successfully deactivated. It then uses a floating contact to activate the alarm system externally (compelled signaling). The light emitting diodes of the activation units signal this by lighting for 2.5 seconds. The light emitting diode(s) on the deactivation unit(s) go out. **The BAS** acoustically signals – for example, on the activation unit – that the system has been successfully activated.

Switching off the alarm system

The person with switching authorization again presses his or her transponder twice in quick succession within transmitting range of the activation unit. The deactivation units signal this to the digital locking cylinders or the digital Smart Relays. The LEDs on the activation units visually signal that the system has been successfully deactivated by blinking 1x short-long. The LEDs on the deactivation unit(s) light again. (The LEDs on the deactivation units are used only for testing purposes, so they do not have to be brought out where they can be seen). Now it is possible to access the doors again with all authorized transponders.

☺ By simply clicking the transponder button within transmitting range of activation units, you can determine the activation state of the alarm system if the LEDs on the activation units are brought out where they can be seen. 1 x short-long blinking means "deactivated", 1 x long (2.5 sec.) blinking means "activated".

Activation transponder

For emergencies, you can use the locking plan software to program a transponder that cancels the deactivation of the locking cylinder so that the doors can be opened with an authorized transponder. However the alarm system remains activated **externally.**

Time zone control und access logging

The activation units (master and slaves) can log activation/deactivation switches (access logging), and you can define time slots during which it is possible to activate/deactivate the system (time zone control):

Access logging	The activation unit stores the last 128 activations/deactivations with date, time and the user name of the transponder. You can read out the data with the programming device or over the network.
Time zone control	You can program activation units in such a way that authorized transponders can only switch the alarm system at certain times.

Refer to the Software Operating Instructions, timezone admiinistration

1.2 Safety Remarks

- Read through the assembly instructions carefully and thoroughly before installing and commissioning the Shunt lock components. They contain important information on the assembly, programming and operation.
- The components are built in accordance with the latest state of the technology. Use them only as instructed and when they are in perfect technical condition and are properly installed according to the technical specifications
- The manufacturer is not liable for damages that are caused by use that does not comply with the directions.
- Keep the documentation that comes with the product and system-specific notices in a safe place.
- Only trained experts are authorized to perform installation, programming and repair work.
- Soldering and connection work anywhere in the entire system must be performed only when the system is voltage-free.
- Soldering work must be performed with a temperature-controlled soldering iron that is electrically insulated from the power system.
- Observe VDE safety regulations and regulations from the local electric utility.
- Do not use the components in areas subject to explosion hazards or in areas with fumes that dissolve metal or plastic.
- DIN norms and the guidelines of VdS Class C must be adhered to.

2.0 Assembly Instructions

2.1 General Information on Installing the Components

Always install in the protected area, for example, in the inside area behind the door, behind brickwork, etc. There are some materials, however, such as stainless steel or aluminum, that can significantly reduce the range. There may also be sources of magnetic interference near the activation or deactivation unit that also very strongly reduce the range. When making the connections, please observe the technical specifications for the activation unit and the relay (refer to Chap. 6). Failing to comply with these values can lead to interference with the function of the components or even to destruction of the components. **Make absolutely sure that the polarity is correct.** You can attach the components (deactivation and activation units) on the wall surface with two countersunk head screws, 3.5 x 30 mm, and two S5 plastic plugs (not included in the delivery).
The two enclosed VdS adhesive labels guarantee permanent evidence if the housing is opened without authorization (sealing of the cover screws).

Programming the components

Program the Shunt lock components and accompanying lockings before installation. When doing this, please keep the following points in mind:

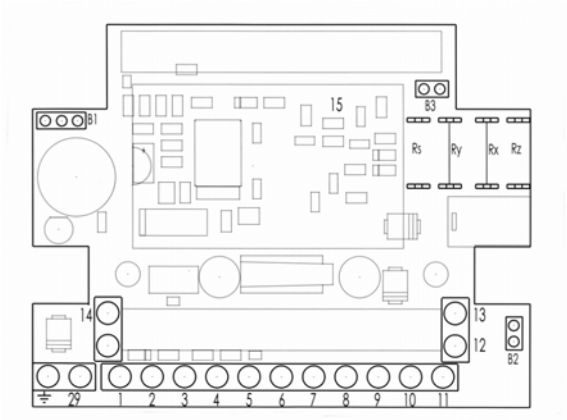
- Program activation units, deactivation units and locking cylinders in the same locking plan
- Select type C*ontrol unit* for the shunt lock components
- During programming, supply only one component with power at a time and do not connect the cables to one another.
- After programming, read out the components and verify that they report correctly.

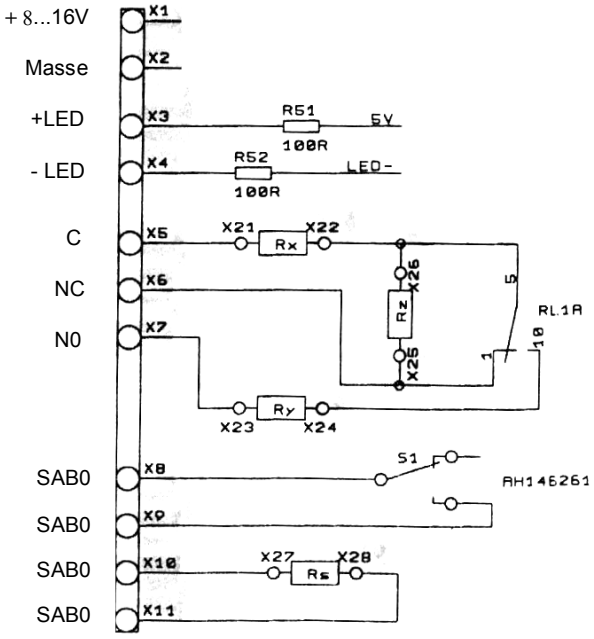
Refer to Chapter 3 for more detailed information.

Installing a locking that should be deactivated with the Shunt lock function

Install the digital locking (Smart Relay or locking cylinder) that should be deactivated by the Shunt lock function. **Follow the installation guidelines. These are under the relevant heading in the system manual.**

2.2 Installing the Deactivation Unit (DA)





Soldering terminal assignments:

1	Supply voltage positive pole
2	Supply voltage negative pole (ground)
3 + 4	Connection for LED (5 volts) in outside area
5 - 7	Not used
8 - 11	Sabotage contacts
12	Optional lock monitoring contact for activation suppression
13	Deactivation request (input)
14	Deactivation acknowledgement (output)
15	Ground (identical to soldering terminal 2)
29	Acoustic BAC acknowledgement **(not for DA)**
30	Solder terminal for cable screen

Jumper settings:

Jumper B1 can be inserted any way
Insert jumper B2 for maximum transmitting range
Do not insert jumper B3

2.2.1 Testing the Deactivation Unit (DA):

To test, connect the deactivation unit to a 9-volt compound battery. Make sure that the polarity is correct. Position the deactivation unit within radio range of the digital locking:

Deactivation unit → digital locking cylinder max. 40 cm (16 inches)
Deactivation unit → digital Smart Relay min. 20 cm, max. 1 m (8 till 40 inches)

The ranges depend on the structural circumstances and so will vary.

Make sure that both the deactivation unit and cylinder are correctly programmed (refer to Chapter 3). Then connect soldering terminals 13 and 15 (ground) to one another. This deactivates the cylinder/Smart Relay (signal tone for cylinder) and the LED on the deactivation unit goes out. The cylinder no longer responds to transponders. When you remove the connection, the cylinder or Smart Relay is activated. The LED lights again. Repeat the tests several times until the radio link works perfectly.

☺ You can increase the range between the cylinder and deactivation unit by using FH version locking cylinders (with plastic inside knob).

Once the deactivation unit successfully passes the test, you can carry out the actual permanent installation.

2.2.2 Connecting Power Supply, Lock Contact Evaluation and Sabotage Contacts:

- Power supply

Connect the positive pole of a direct current source between +8 ... + 16 V (recommended: +12 V) to soldering terminal 1. Note that the voltage is not permitted to
exceed a value of +16 V under any circumstances.
Connect soldering terminal 2 to ground.

- Optional lock contact evaluation (global activation suppression)

If you want the alarm system to remain inactivated until all doors of the security area are closed, meaning the bolts have been driven out, you can connect the lock switch contact to soldering terminals 12 and 15. The lock contact must be a floating electric strike.

☺ If there is no lock contact (not VdS-compliant), it is, of course, impossible to check whether all doors have been locked, which means that it is also possible to activate the alarm system if some doors are not locked. In any case, however, all cylinders must have been successfully deactivated.
If there is no lock contact, simply do not connect soldering terminals 12 and 15.

Test the shunt lock function again after you have connected the lock switch contact. Try to deactivate the locking cylinder or Smart Relay even when the bolts have not been driven out.

- External light emitting diode

You can connect an external light emitting diode to soldering terminals 3 and 4 so that you have a visual display in the outside area showing whether the cylinder or Smart Relay is activated or deactivated. Maximum length of the line: 10 m (33 feet).

- Switch contacts (not used)

Soldering terminals 5 to 7 are not needed for the deactivation unit.

- Sabotage contacts

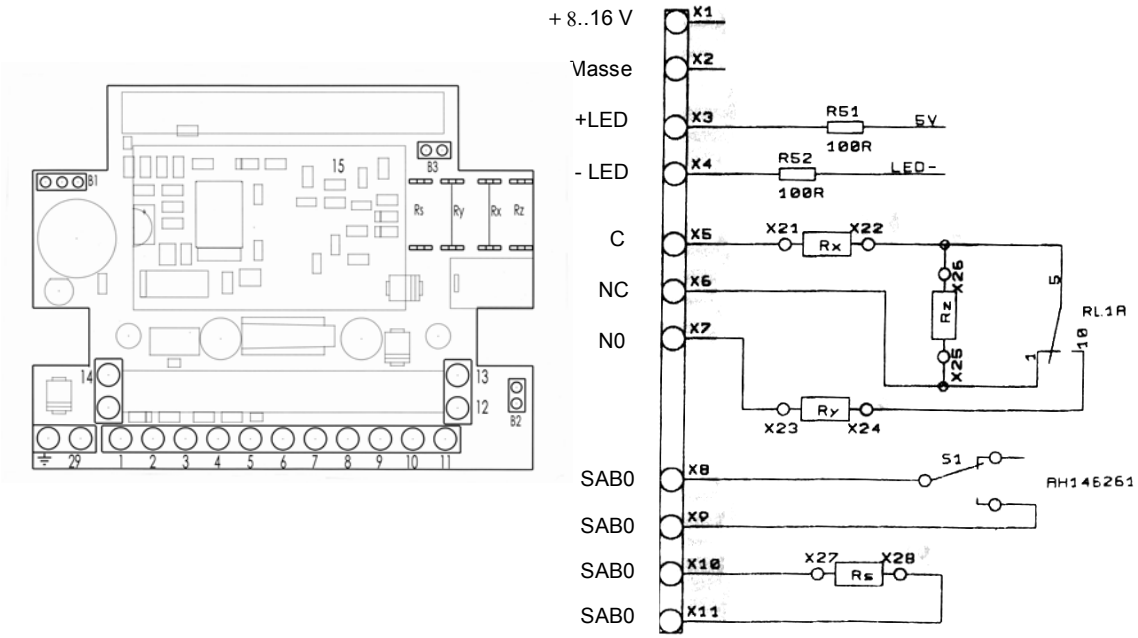
Connect these to soldering terminals 8 to 11. Solder the Rs resistor (terminating resistor or short circuit) to soldering pins X27 and X28 (refer to the drawing).

Install other deactivation units, if any, according to the same plan.

2.2.3 Connecting Deactivation Request and Deactivation Acknowledgement

Refer to Chapter 2.5

2.3 Installing the Master Activation Unit (MA)



Soldering terminal assignments:

1	Supply voltage positive pole
2	Supply voltage negative pole (ground)
3 + 4	Connection for LED (5 volts) in outside area
5 - 7	Floating contacts for switching the alarm system
8 - 11	Sabotage contacts
12	Activation request from slave activation units (SAs) (optional)
13	Deactivation acknowledgement (input) → Activation suppression when ground is applied
14	Deactivation request (output)
15	Ground (identical to soldering terminal 2)
29	Acoustic activation acknowledgement by BAC (not for DA)
30	Solder terminal for cable screen

Jumper settings:

Jumper connects right and middle contacts of B1:
⇒ Acoustic acknowledgement after activation release by activation unit

Jumper connects left and middle contacts of B1:
⇒ Acoustic acknowledgement after final activation is done by the BAC (this is the VdS-compliant configuration).

The BAC must draw pin 29 to ground for the acoustic acknowledgement.

Jumper B2 is inserted:

⇒ Maximum transmitting range. For VdS-compliant installation, however, you must then work with external keys to differentiate between outside and inside. (refer to 4.3 VdS-Compliant Installation of the Activation Unit).

⇒ In VdS-compliant installation, the range of the antenna extender is reduced solely by the correct use of the aluminum sleeve. (Refer to 4.3 VdS-Compliant Installation of the Activation Unit).

Install the activation unit so that the distance between its antenna and other digital components is **at least 1 m (40 inches).**

2.3.1 Testing the Master Activation Unit (MA):

Before final installation, apply voltage to contacts 1 and 2 of the activation unit (compound battery). Make sure that the polarity is correct. Do not wire the other contacts for this test.

Transponder → master activation unit **1 cm to max. 3 cm (.4 to 1.2 inches)**

ⓘ This corresponds to the strongly reduced range when the screening sleeve is inserted on the antenna extender (refer to Chap. 4.3).

Make sure that all components are correctly programmed (refer to Chap. 3). Insert jumper B1 on the right. Then test whether the relay on the activation unit switches (soldering terminals 5 and 7) by operating the transponder two times in quick succession (within 0.5 ... 2 sec.).
An acoustic signal indicates the switching state of the alarm system. A 2.5-second long continuous tone signals that the activation contact was closed and a two-part signal tone (short – long) means that the activation contact is open again (de-activated).

Then you must convert the acoustic activation acknowledgement to BAC operation (insert jumper B1 to the left) and test it by attempting to activate the system. Once the master activation unit has successfully passed the test, you can carry out the actual permanent installation.

2.3.2 Connecting Power Supply, Switch Contacts and Sabotage Contacts:

- <u>Power supply</u>

Connect the positive pole of a direct current source between +8 ... + 16 V (recommended: +12 V) to soldering terminal 1. Note that the voltage is not permitted to
exceed a value of
+16 V under any circumstances
Connect soldering terminal 2 to ground

- External light emitting diode

You can connect an external light emitting diode to soldering terminals 3 and 4 for visual signaling. When the transponder is operated successfully, the LED blinks. Maximum length of the line: 10 m (33 feet).

- Switch contacts

Connect them to the alarm system. Soldering terminal 5 is the common contact, 6 is for the electric strike and 7 for the make contact. Refer to the BAS installer instructions for the wiring and values for the terminating resistor(s).
Rx: wire jumper; Ry: wire jumper; Rz: terminating resistor

- Sabotage contacts

Connect them to soldering terminals 8 to 11. Solder the Rs resistor (terminating resistor or short circuit) to soldering pins X27 and X28 (refer to the drawing).

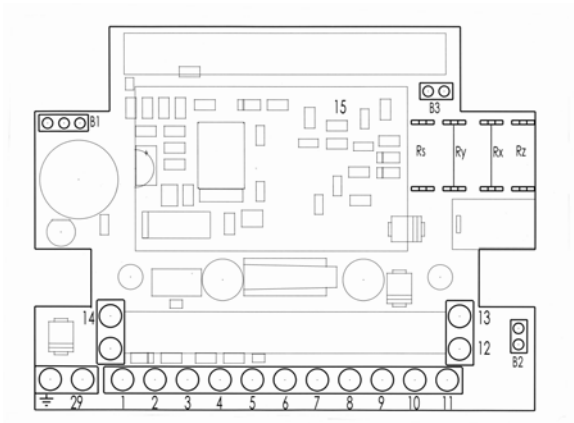
- Global activation suppression (optional)

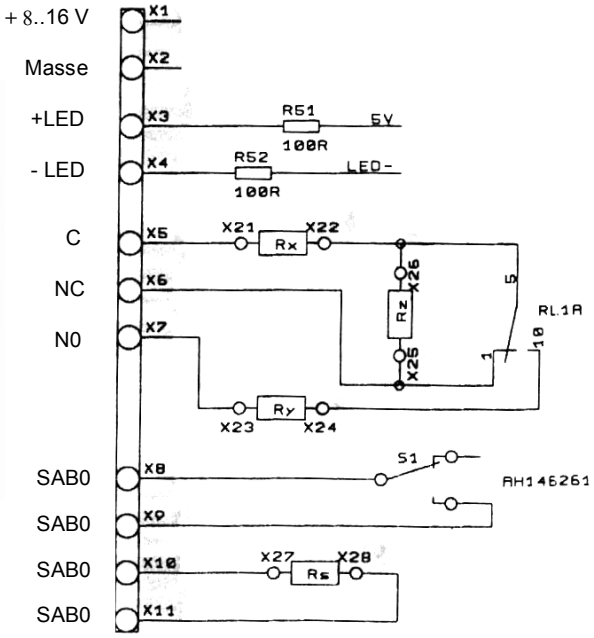
Applies ground (such as pin 15 or pin 2) to pin 13 over a floating contact so that the system cannot be activated.

2.3.3 Connecting Deactivation Request, Deactivation Acknowledgement and Activation Request

Refer to Chapter 2.5.

2.4 Installing the Slave Activation Unit (SA)





Soldering terminal assignments:

1	Supply voltage positive pole
2	Supply voltage negative pole (ground)
3 + 4	Connection for LED (5 volts) in outside area
5 - 7	Not used
8 - 11	Sabotage contacts
12	Optional activation suppression when ground is applied (for example, lock contact evaluation)
13	Deactivation acknowledgement (input)
14	Activation request to the master activation unit MA (output)
15	Ground (identical to soldering terminal 2)
29	Acoustic activation acknowledgement by BAC (not for DA)
30	Solder terminal for cable screen

Jumper settings:

Jumper connects right and middle contacts of B1:

⇒ Acoustic acknowledgement after activation release by activation unit

Jumper connects left and middle contacts of B1:

⇒ Acoustic acknowledgement after final activation is done by the BAC. The BAC must draw pin 29 to ground (VdS-compliant configuration).

Jumper B2 is inserted:

⇒ Maximum transmitting range. For VdS-compliant installation, however, you must then work with external keys to differentiate between outside and inside. (Refer to 4.3 VdS-Compliant Installation of the Activation Unit).

⇒ In VdS-compliant installation, the range of the antenna extender is reduced solely by the correct use of the aluminum sleeve. (Refer to 4.3 VdS-Compliant Installation of the Activation Unit).

2.4.1 Testing the Slave Activation Unit (SA):

Before final installation, apply voltage to contacts 1 and 2 of the activation unit (compound battery). Make sure that the polarity is correct. Do not wire the other contacts for this test.

Transponder → slave activation unit **1 cm to max. 3 cm (.4 to 1.2 inches)**

ⓘ This corresponds to the strongly reduced range when the screening sleeve is inserted on the antenna extender (refer to Chap. 4.3).

Make sure that all components are correctly programmed (refer to Chap. 3). Insert jumper B1 on the right. Then test whether the relay on the activation unit switches (soldering terminals 5 and 7) by operating the transponder two times in quick succession (within 0.5 ... 2 sec.).

Then you must convert the acoustic activation acknowledgement to BAC operation (insert jumper B1on the left) and test it by attempting to activate the system. Once the slave activation unit successfully passes the test, you can carry out the actual permanent installation.

2.4.2 Connecting Power Supply, Sabotage Contacts and Local Activation Suppression:

- Power supply

Connect the positive pole of a direct current source between +8 ... + 16 V (recommended: +12 V) to soldering terminal 1. Note that the voltage is not permitted to
exceed a value of +16 V under any circumstances.
Connect soldering terminal 2 to ground.

- External light emitting diode

You can connect an external light emitting diode to soldering terminals 3 and 4 for visual signaling. When the transponder is operated successfully, the LED blinks. Maximum length of the line: 10 m (33 feet).

- Switch contacts

Soldering terminal 5 to 7 are not needed for the slave activation unit unless you want to use the SA for internal activation. In this case, wire the SA separately from other activation units. Connect soldering terminals 5 to 7 to the internal activation connection of the BAC. Refer to the BAS installer instructions for wiring information.

- Sabotage contacts

Connect them to soldering terminals 8 to 11. Solder the Rs resistor (terminating resistor or short circuit) to soldering pins X27 and X28 (refer to the drawing).

- Optional local activation suppression

If you want to use activation suppression, connect a floating contact between soldering terminals 12 and 15. When the contact is closed, it is impossible to activate or deactivate the system locally (from this SA). This has no effect on the activation behavior of other activation units.

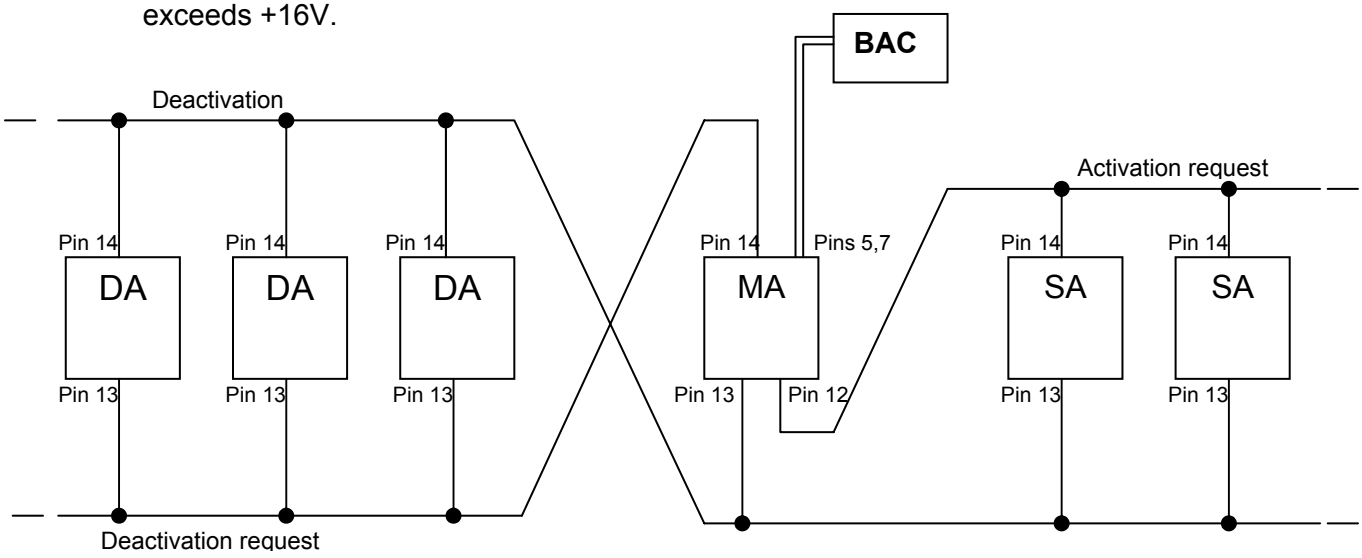
2.4.3 Connecting Deactivation Acknowledgement and Activation Request

Refer to Chapter 2.5.

2.5 Wiring the Shunt Lock Components

We recommend that you use the following types of lines: J-Y(ST)Y 6 or 8 pin, Ø 0.6 mm. The diameter should be fit to the length of the line so that the minimum voltage for the components never falls below +8 volt (voltage drop on the line).
ATTENTION: You should always shield longer lines.

Connect the deactivation request, deactivation acknowledgement and activation request to one another according to the drawing below.
Also connect the supply voltage everywhere (pins 1 and 2, with the positive on 1 and ground on 2). Make sure that the polarity is correct. Then measure the voltage on all units and make sure that the voltage never falls below a value of +8v and never exceeds +16V.



	DA	MA	SA
Deactivation request	Solder pin 13	Solder pin 14	-
Deactivation acknowledgement	Solder pin 14	Solder pin 13	Solder pin 13
Activation request	-	Solder pin 12	Solder pin 14
Activation suppression	Solder pin 12	-	Solder pin 12
Supply voltage positive	Solder pin 1	Solder pin 1	Solder pin 1
Supply voltage ground	Solder pin 2	Solder pin 2	Solder pin 2

DA = Deactivation unit
MA = Master activation unit
SA = Slave activation unit

2.6 Functional Principles

1. A DA deactivates a neighboring cylinder if the deactivation request line (pin 13) is drawn to ground potential by the MA **or** the BAC.

2. A DA reactivates a neighboring cylinder as soon as the deactivation request line (pin 13) is high-impedance, which means that the MA output (pin 14) and the corresponding BAC output must **both** be high-impedance.

3. A DA draws the deactivation acknowledgement line (pin 14) to ground as long as its neighboring cylinder is activated or as long as the lock monitoring input (pin 12) is connected to ground. Therefore, a lock contact must be an electric strike between ground and pin 12 that opens when the bolt is pushed forward.

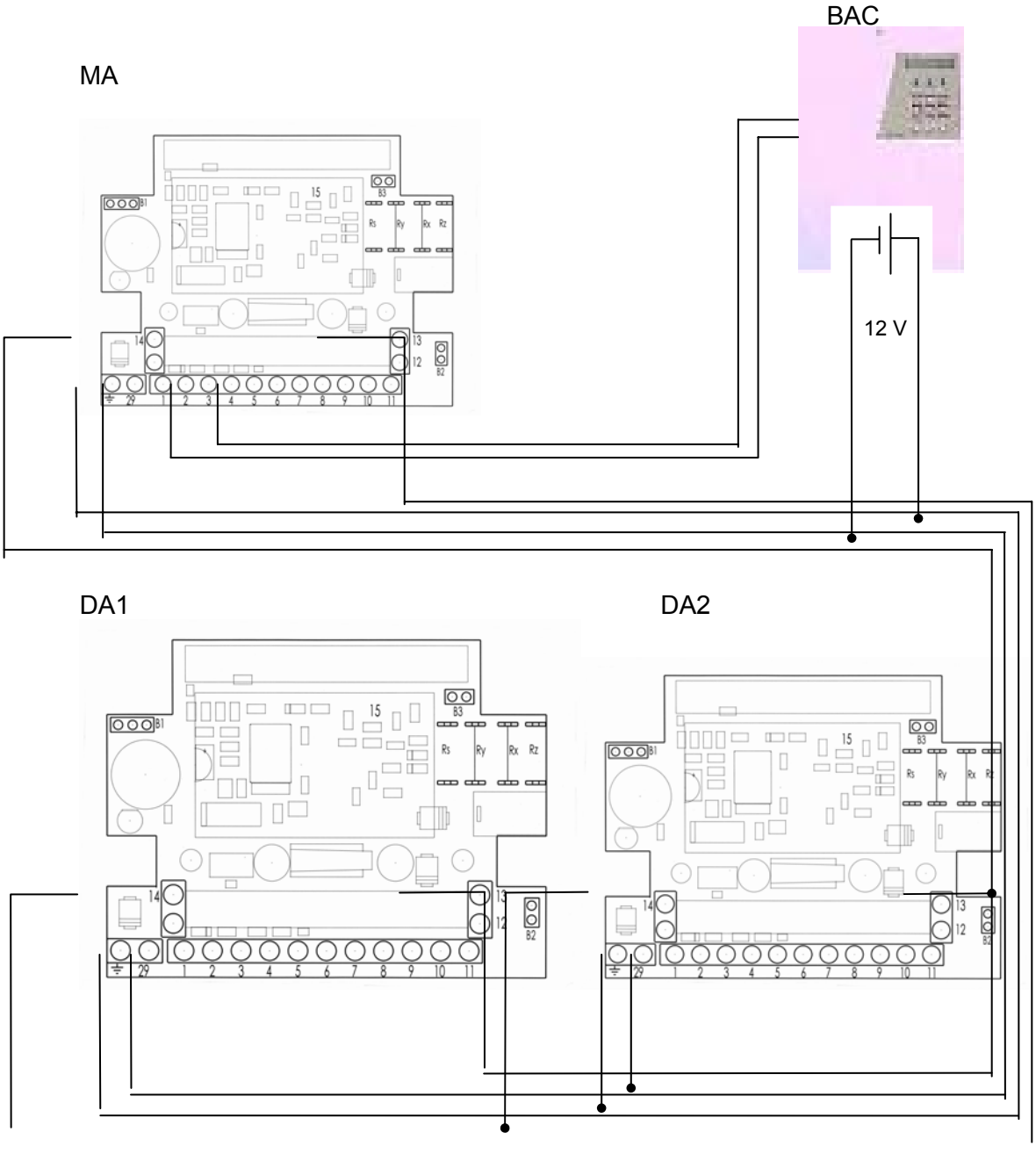
4. Consequently, the deactivation acknowledgement line does not go to high-impedance until each deactivation unit has successfully deactivated its neighboring cylinder and, if there is lock contact evaluation, all bolts have been pushed forward.

5. An MA draws the deactivation request line (pin 14) to ground potential after someone authorized to activate the system operates the transponder.
   This causes each DA to start to deactivate its cylinder.
   If the MA receives a positive deactivation acknowledgement within no more than 10 sec. (deactivation acknowledgement line goes high-impedance), a floating contact is closed between pin 5 and pin 7. This requests the BAC to activate the system.

6. When someone authorized to activate the system operates the transponder again, the floating contact between pins 5 and 7 is separated immediately, so that the BAC is requested to deactivate.
   Then the deactivation request line (pin 14) is set to high-impedance. The DAs then start to reactivate unless the BAC continues to draw the deactivation request line to ground potential in order to prevent the cylinders from reactivating (for example, until the system deactivation is complete).

7. Instead of operating the transponder at the MA, the slave activation units (after transponder activation at the SA by someone authorized to activate the system) can trigger an activation or deactivation process with a "high-impedance – ground potential – high-impedance" pulse on the activation request line (pin 14).

Connecting plan (example with one MA and 2 DAs)



After you have completed the installation work, carry out a function test.

Do this by operating an authorized transponder near the activation unit twice in quick succession. The light emitting diodes on the activation unit and the deactivation unit(s) go out and you receive the acoustic acknowledgement signal from the BAC or (if jumper B1 is inserted on the right) the signal lasting 2.5 seconds from the activation unit indicating that the alarm system has been activated.

Check whether the cylinder(s) or Smart Relay(s) have been deactivated.

Operate the transponder near the activation unit two times again. This unit signals the activation of the lockings only visually on the LED with 1 x short-long blinking or (if jumper B1 is inserted on the right) with a double signal tone from the activation unit. The LEDs on the shunt lock components light again.

The locking cylinder or Smart Relay is now active and can be switched if you operate an authorized transponder one time.

Please set the acoustic activation acknowledgement to BAC operation (insert jumper B1 on the left) if you have not done this yet.

Test the Shunt lock function several times.

3.0 Programming

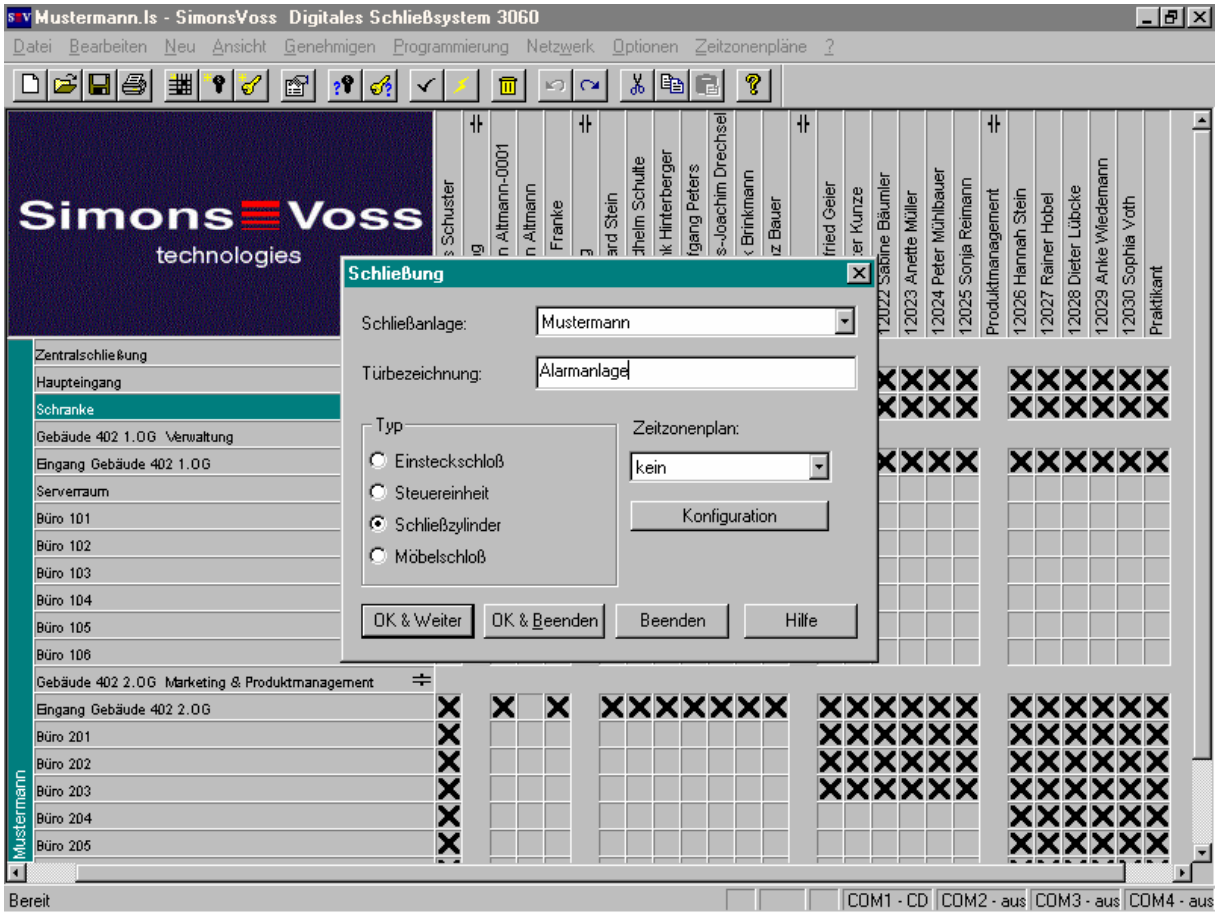
3.1 Programming the Activation Units (MA and SA)

If you want to add the shunt lock components at some time after the initial installation, open your locking plan with the password. If this is the initial installation, create a new locking plan.

Click the locking above which you want to add an activation unit. Select **New** → **Locking**. Then give the activation unit a name:

➲ For example, Alarm system

In the field **Type**, select C*ontrol unit.* Click **OK & Exit** or **OK & Next**, if you want to set up additional activation units (slaves).

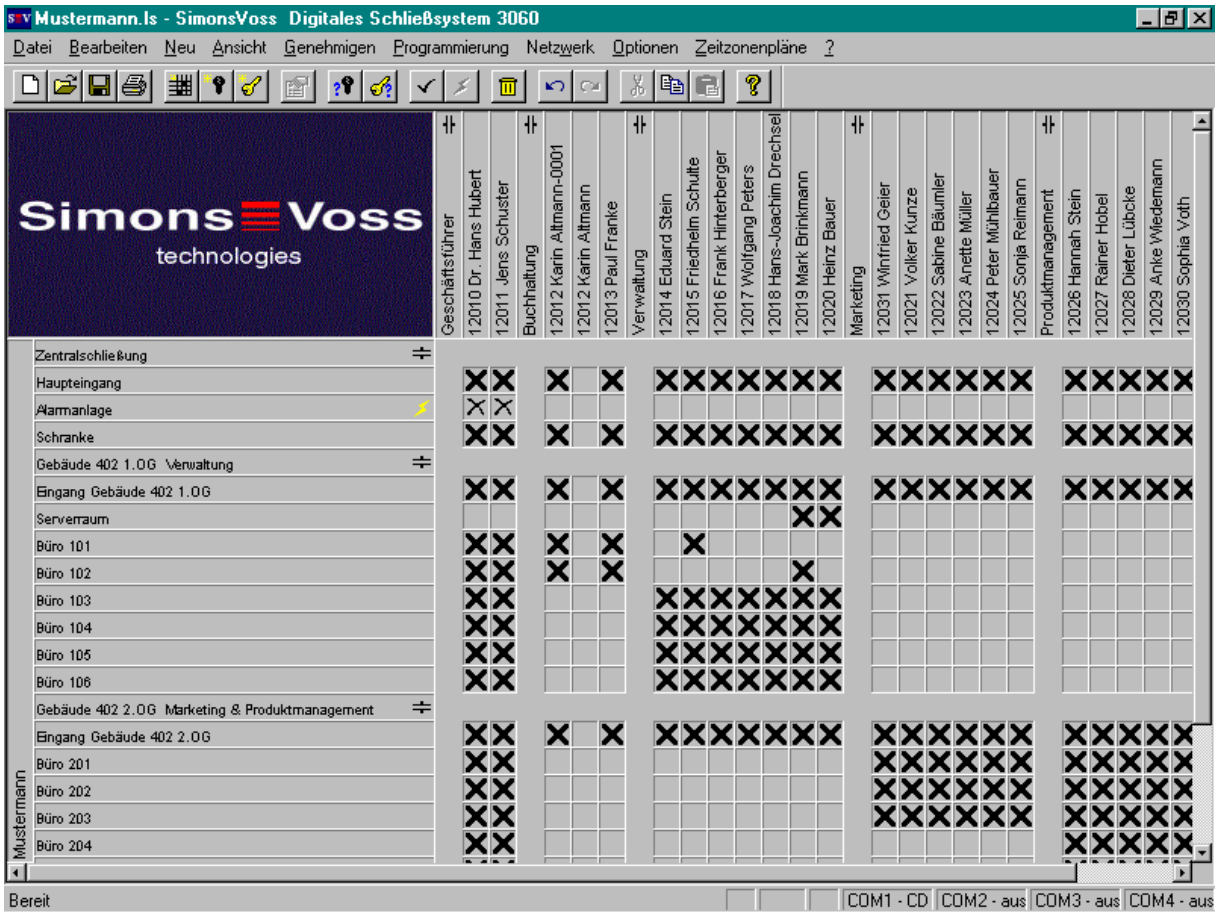


In the locking plan, make a cross by the employees who are authorized to turn the alarm system on and off.

☺ You do not have to reprogram the transponders in this case.

Approve your locking system and program the activation unit under **Programming** → **Locking**.

☝ The activation unit needs supply voltage during the programming. You can provide this with a 9-volt compound battery, for example. Program activation unit(s) and deactivation units separately from one another. Do not wire the two components until after you have programmed them successfully.



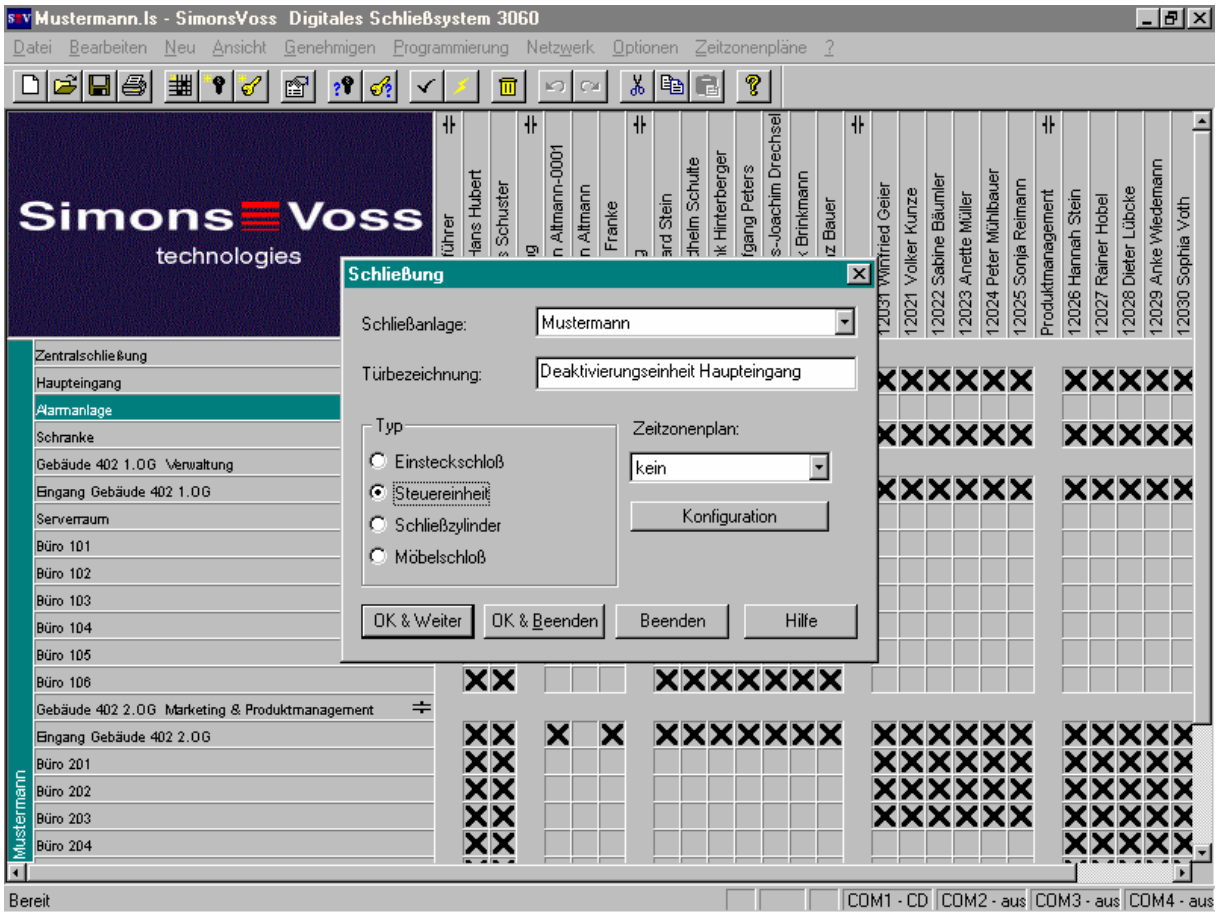
3.2 Programming the Deactivation Units (DA)

Click the line in the locking plan above the one where you want to add a deactivation unit. Select **New** → **Locking**. Then give the deactivation unit a name:

➲ Such as Deactivation unit, main entrance

In the field **Type**, select *Control unit*. Click **OK & Exit**. If you want to set up additional deactivation units, repeat these steps.

☺ If you always add the deactivation units above the accompanying digital locking cylinder, you will have a better overview of the system.

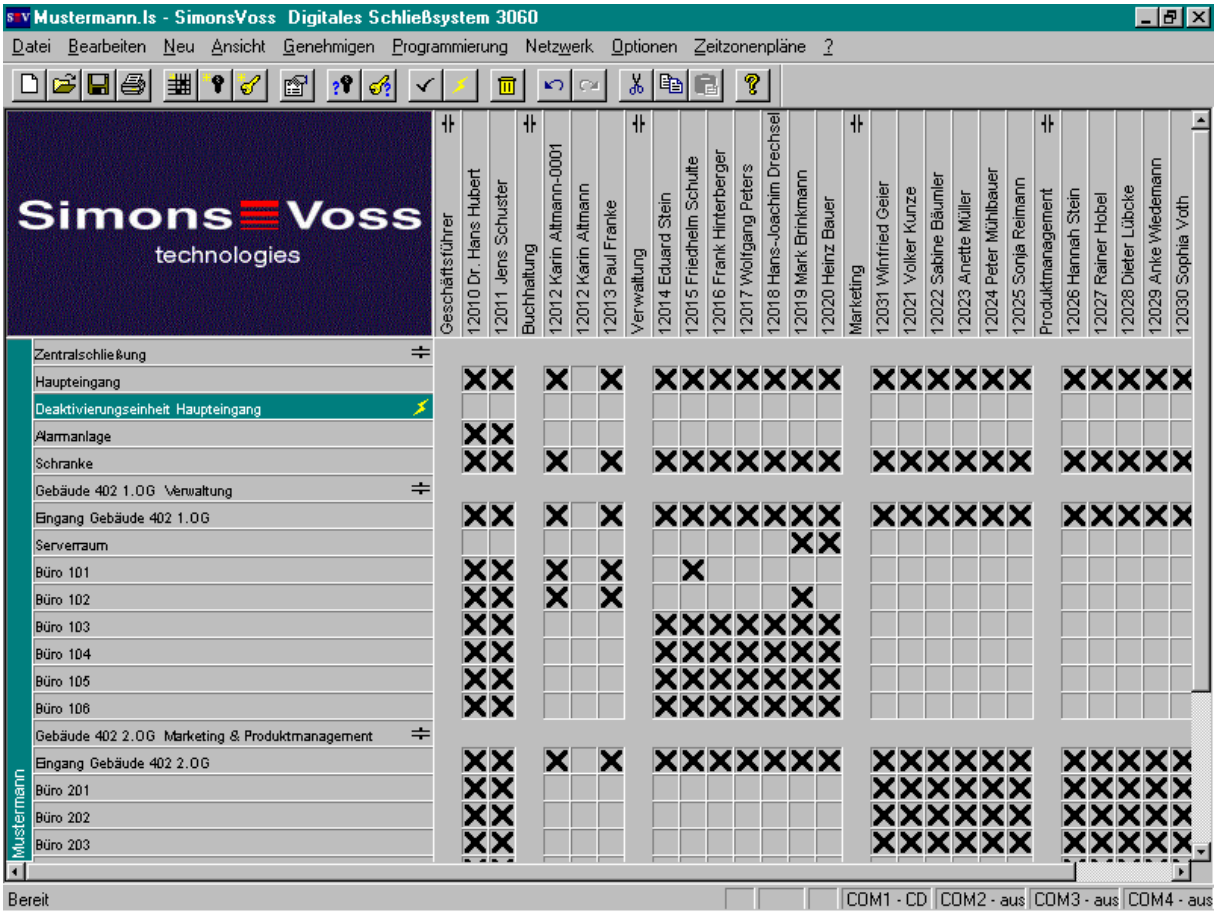


Deactivation units do not need any authorizations which means that you do not have to insert any crosses. Approve your locking system and program the deactivation units under **Programming** → **Locking**.

☝ The deactivation unit needs supply voltage during the programming. You can provide this with a 9-volt compound battery, for example. Program activation unit(s) and deactivation units separately from one another. Do not wire the two components until after you have programmed them successfully.

Read out the shunt lock components: **Programming → Read unknown locking**. The type of the component (deactivation unit or activation unit) is displayed.

Attention: The display treats slave activation units as normal control unit.

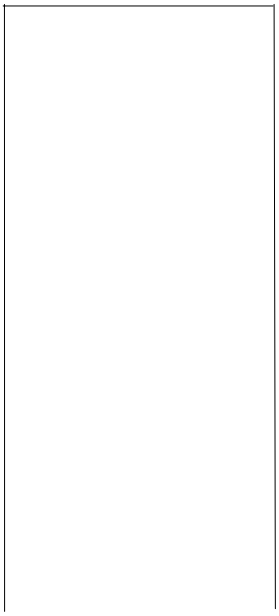


4.0 Installation

4.1 Installing the Deactivation Unit

Install the deactivation unit DA in the immediate vicinity of the digital locking cylinder (no farther than approximately 30 cm or 12 inches). This guarantees optimum transmission traffic. Align the deactivation unit so that both fastening screws lie in a horizontal line. Then the antennas point directly to the locking cylinder (refer to the drawing below).

☺ You can always achieve better ranges if you use FH cylinders (plastic knob instead of stainless steel).

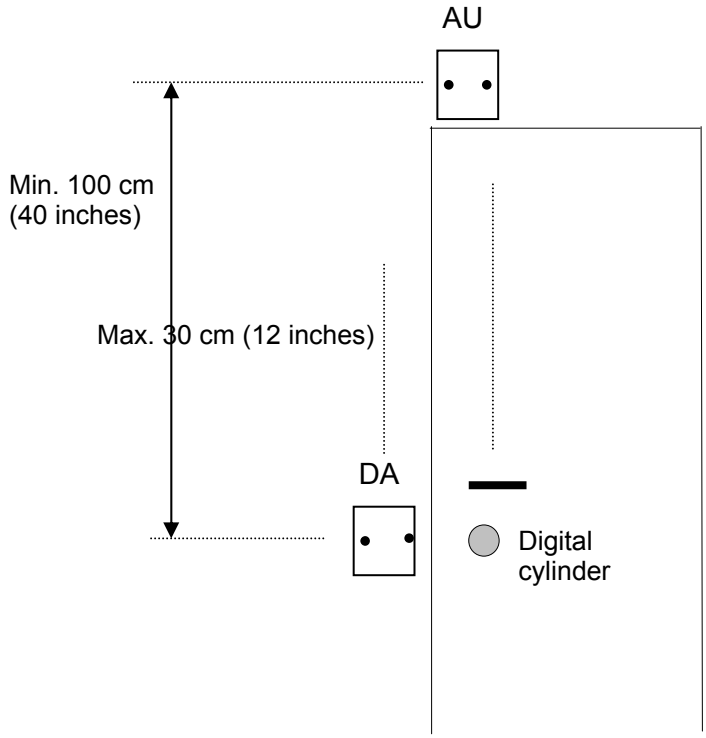


4.2 Installing the Activation Unit (MA and SA)

You should install the activation unit (AU), no matter whether it is a master activation unit MA or slave activation unit (SA), above the door case and above the locking cylinder. In any case, the distance to other SimonsVoss components **must** be at least 1 m or approximately 40 inches (refer to the drawing).
Only in this way can you rule out mutual interference influences.

If you install it above the door case, align the activation unit so that the two fastening screws lie in a horizontal line. This eliminates interference when the door is used in the normal way. (Refer to the drawing below.)

This installation is done without the antenna extender and with jumper B2 is inserted (max. range). Because this (simple) installation method allows the system t



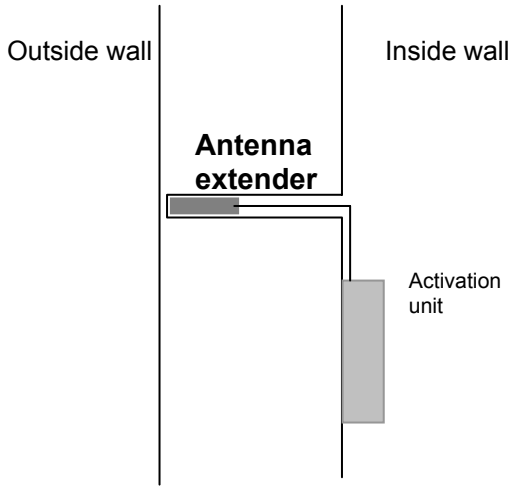
4.3 VdS-Compliant Installation of the Activation Unit (MA and SA)

VdS-compliant installation must guarantee that the system can be activated from the outside, but not from the inside. This requires the following measures:

3. Use **activation units with antenna extender.** Shorten the color-coded cable on the antenna extender to the required length, pull the cable through the bore hole in the aluminum screening sleeve and connect the cable to soldering connections 16 to 20 as follows:
   16 - green, 17 - blue, 18 - screening, 19 - red, 20 - yellow.

4. **Insert jumper B2!** The range of the antennas is reduced if you use the aluminum sleeve correctly.
   Bore a blind hole (∅ 23 mm) in the outside wall, insert the antenna extender in the blind hole and fix in position. (See drawing below). While doing this, make sure that you get within at least 2 cm (approximately 3/4 inch) of the front side of the antenna extender from the outside and that you guarantee a minimum distance of at least 12 cm (4 3/4 inches) to the front side of the antenna extender from the inside. This is approximately the thickness of the wall.
   The distance between the antenna and activation unit must be at least 30 cm (12 inches) and the distance from the locking cylinder to the antenna must be at least 1 m (40 inches).

5. We recommend that you mark the position of the blind hole on the outside wall with a red point or similar marking. The person authorized to activate the system must hold the transponder at this point in order to be able to communicate with the antenna extender.



6. Install the deactivation unit according to the description in Chapter 4.1.

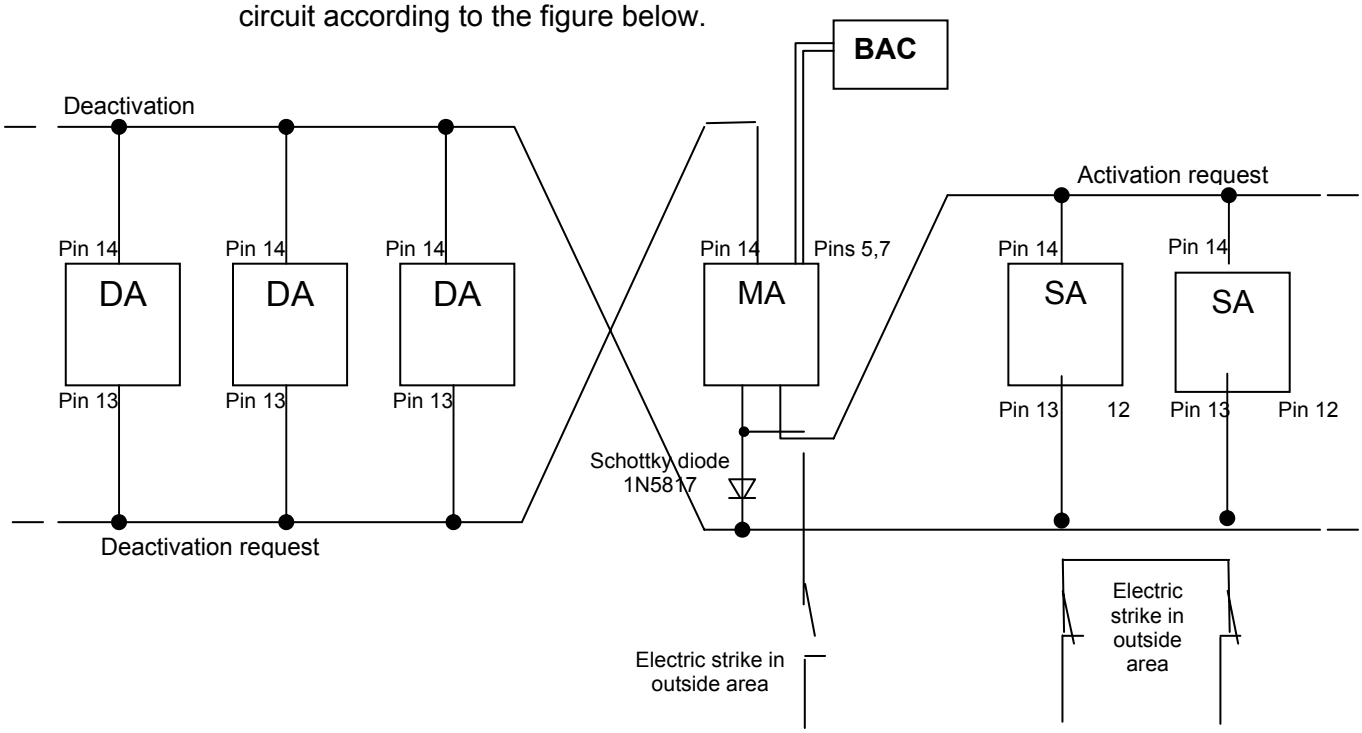
7. You can also **optionally** use an **activation unit without antenna extender.** Install it as described in Chapter 4.2.

   In order to guarantee that the system can be **externally activated** from the outside only, you must then install a **button in the outside area.** You cannot externally activate or deactivate the system by operating a transponder until this button is pushed.

   The deactivation acknowledgement input (pin 13) is suppressed on master activation units (MAs) as long as it is connected to ground (normally closed button in outside area).

   A Schottky diode decouples the deactivation acknowledgement line (see below). This diode is needed, however, only if there are slave activation units.

   With slave activation units (SAs), you can apply the activation suppression (pin 12) to ground over a normally-closed button that is in the outside area. If there is also an activation suppression button on the master, you should use a circuit according to the figure below.



5.0 Special Versions of the Shunt lock function 3066

5.1 Operating the Activation Unit without a Deactivation Unit

If you want to activate and deactivate the burglar alarm system externally with the transponder instead of with a key, you only need a master activation unit (MA). In this case, however, you will lose the true purpose of the Shunt lock function.

👍 You need to connect only pins 1 and 2 for the power supply, the floating switch contact (pins 5, 6, 7) and the sabotage contacts (pins 8 to 11). Do not connect the other lines of the activation unit (refer to Chapter 2.3).

5.2 Operating the Deactivation Unit without an Activation Unit

If you continue to operate the alarm system with a standard key, you can do without the activation unit.

Connection assignment

Connect the supply voltage (separate power supply) to soldering terminals 1 and 2. Connect terminals 13 and 15 over a relay contact of the alarm system (floating make contact). If there is a lock switch contact, wire this to soldering terminals 12 and 15 (Refer to Chapter 2.2).

☺ As long as soldering terminals 13 and 15 are connected to one another, for example, by a relay point of the alarm system, all digital locking cylinders equipped with a deactivation unit are deactivated. This means it is not possible to accidentally go through these doors when the alarm system is activated.

6.0 Data Sheet

MA, SA and DA	Operating voltage Current consumption	8 to 16 volts DC < 30 mA
Applied relay for switching output	Max. continuous current Max. switch on current Max. switching voltage Max. switching capacity	1 A 1 A 40 V AC 30 W / 60 VA
Tamper contact	Make contact	1 A / 30 V DC
Transponder range with extended antenna		1 - 3 cm (.4 to 1.2 inches)
Extended antenna Dimensions Cabel length		 64 x 18 mm 5 m
Temperature range	-10°C to +55°C (14°F to +131°F)	
Degree of protection	VdS environmental class II	
Housing	Material Color Dimensions [L/W/H]	S-B or A-B-S White 85 x 85 x 26 mm
	Article description	_____
	Article number	_____
	VdS no.	G 101 160

Shunt lock function 3066

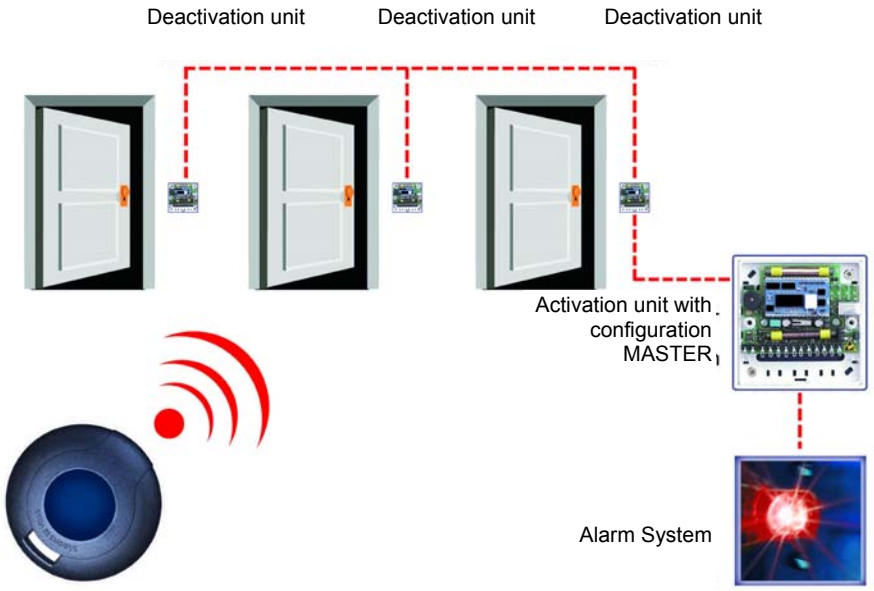
Operator Instructions

Version: January 2004

SimonsVoss technologies

VdS Shunt lock function 3066

Content



1.0 Shunt lock function 3066 System Components _____ 3

2.0 Shunt lock function 3066 Operation _____ 4

3.0 Special Versions of the Shunt lock function 3066 _____ 6

3.1 Operating the Activation Unit without a Deactivation Unit _____ 6

3.2 Operating the Deactivation Unit without an Activation Unit _____ 6

4.0 Data Sheet _____ 7

1.0 Shunt lock function 3066 System Components

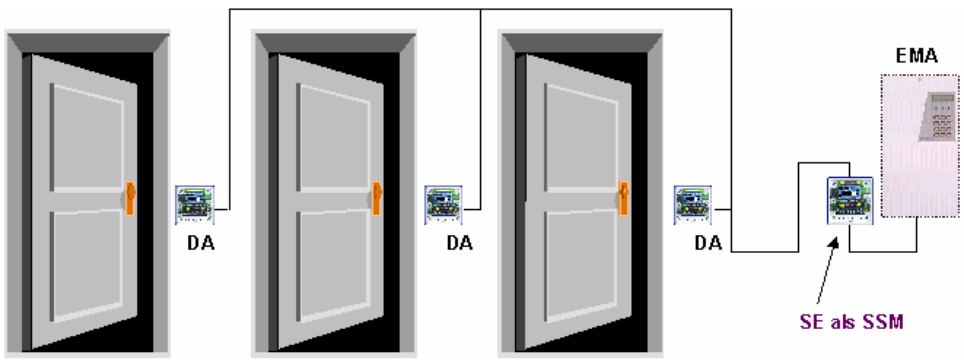
In objects protected by the alarm, measures must be taken to prevent any unintentional entry of the secured area when the alarm system is activated externally (burglar alarm system, BAS) because this would trigger a false alarm. The Shunt lock function 3066 implements such a feature without extensive work on the door or doorframe.

The following components are needed for this:

1. Activation unit(s) (MA and SA)
   Such a unit is used to switch the alarm system. You need at least one activation unit (AU) to activate and deactivate the system externally. If you want
   to be able to activate/deactivate from several locations, you need the corresponding number of activation units. With a mouse click in the locking plan, you can issue the authorizations for activating and deactivating the alarm system.

   Basically, there is a difference between the master activation unit (MA) and the slave activation units (SA). The SAs are needed only if you want to activate/deactivate from more than one location. It is always the MA that activates/deactivates the alarm system externally over a floating contact. SAs only send the appropriate requests to the MA. You can also activate internally by using SAs that are separately connected to the internal activation connection of the burglar alarm center (BAC).

2. Deactivation units (DA)
   These are installed next to the doors of the secured area (and in the immediate vicinity of the digital cylinder). They make sure that even an authorized transponder cannot open these doors accidentally if the alarm system has been activated externally. This reliably prevents false alarms.



2.0 Shunt lock function 3066 Operation

Switching on the alarm system (burglar alarm system, BAS)

The person with switching authorization presses his or her transponder two times in quick succession (within 2 sec.) near an activation unit. This sends a signal to all deactivation units present. If lock contacts are connected to the deactivation units, the DAs first check whether the doors have been correctly locked. The digital locking cylinders or Smart Relays are not deactivated unless this is the case, so that it is no longer possible to enter the secured area. The activation unit does not receive a positive acknowledge until all lockings have been successfully deactivated. It then uses a floating contact to activate the alarm system externally (compelled signaling). The light emitting diodes on the activation units signal this by lighting for 2.5 seconds. The light emitting diode(s) of the deactivation unit(s) go out. The BAS acoustically shows that the activation has occurred - for example, on the activation unit.

Switching off the alarm system

The person with switching authorization again presses his or her transponder twice in quick succession within the transmitting range of the activation unit. The deactivation units signal this to the digital locking cylinders or digital Smart Relays. The BAS acoustically signals the successful deactivation. The LEDs on the activation units signal that the activation has occurred by blinking 1 x short-long. The LEDs on the deactivation unit(s) light again. (The LEDs on the deactivation units are used only for testing purposes, so they do not have to be brought out). Now it is possible to access the doors again with all authorized transponders.

☺ In network operation, (not VdS), you can do without deactivation units. In this case, the network nodes take care of activating and deactivating the locking.

☺ By simply clicking the transponder button within the transmitting range of activation units, you can determine the activation state of the alarm system if the LEDs on the activation units are brought out.

1 x short-long blinking means "deactivated"
1 x long (2.5 sec.) blinking means "activated"

Activation transponder

For emergencies, you can use the locking plan software to program a transponder that cancels the deactivation of the locking cylinder so that the doors can be opened with an authorized transponder. The alarm system, however, remains activated externally and the alarm will be triggered.

- Special model

If you want to keep a log of who switched the alarm system and when, you need an activation unit with access logging (PLUS version).

● PLUS activation unit
Design is similar to the standard version, but with access logging and time zone control.

Access logging	The activation unit stores the last 128 accesses with date, time and the user name of the transponder. You can read out the data with the programming device or over the network.
Time zone control	You can program activation units in such a way that authorized transponders can switch the alarm system at certain times only.

Safety remarks

- Read through the operating manual carefully and thoroughly before putting the shunt lock components into operation. This manual contains important information on operation and programming.
- The components are built in accordance with the latest state of the technology. Use them only as instructed and only when they are in perfect technical condition and are properly installed according to the technical specifications.
- The manufacturer is not liable for damages that are caused by use that does not comply with the directions.
- Keep the documentation that comes with the product and system-specific notices in a safe place.
- Only trained experts are authorized to perform installation, programming and repair work.
- Soldering and connection work within the entire system must be performed only when the system is voltage-free.
- Soldering work must be performed with a temperature-controlled soldering iron that is metallically separated from the power system.
- Observe VDE safety regulations and regulations of the local electric utility.
- Do not use the components in areas subject to explosion hazards or in areas with fumes that dissolve metal or plastic.
- DIN norms and the guidelines of VDS Class C must be adhered to.

3.0 Special Versions of the Shunt lock function 3066

3.1 Operating the Activation Unit without a Deactivation Unit

If you want to activate and deactivate the burglar alarm system externally with the transponder instead of with a key, you only need a master activation unit (MA). In this case, however, you will lose the true purpose of the shunt lock function.

3.2 Operating the Deactivation Unit without an Activation Unit

If you continue to operate the alarm system with a standard key, you can do without the activation unit. In this case, the BAS controls the deactivation units.

Data Sheet

MA, SA and DA	Operating voltage Current consumption	8 to 16 Volts DC < 30 mA
Applied relay for switching output	Max. continuous current Max. switch on current Max. switching voltage Max. switching capacity	1 A 1 A 40 V AC 30 W / 60 VA
Tamper contact	Make contact	1 A / 30 V DC
Transponder range with extended antenna		1 – 3 cm
Temperature range Degree of protection	-10°C to +55°C (14°F to +131°F) VdS environmental class II	
Housing	Material Color Dimensions [L/W/H]	S-B or A-B-S White 85 x 85 x 26 mm
	Article description Article number	_____ _____

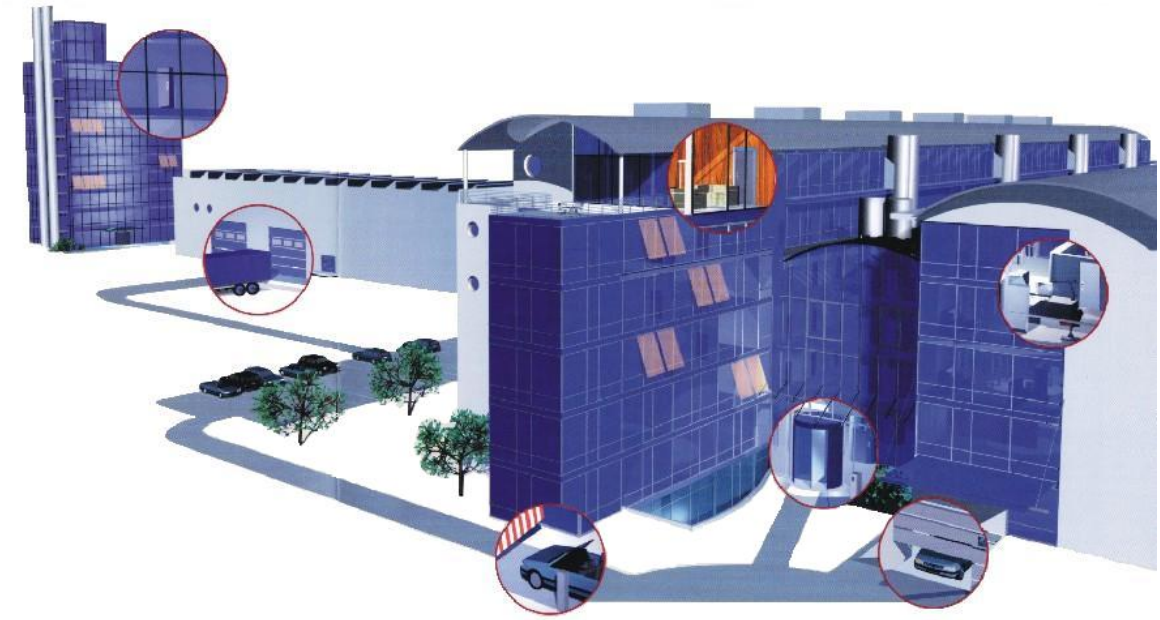
WAVENET
RADIO NETWORK 3065

Status: August 2007

SimonsVoss technologies

WAVENET RADIO NETWORK 3065

Table of Contents



1.0 INTRODUCTION. 5
2.0 NOMENCLATURE. 6
3.0 TRANSMISSION MEDIA. 7
4.0 USABLE RADIO BANDS. 8
5.0 WHAT ARE THE BASIC INFLUENCING FACTORS? 9
6.0 SECURITY OF TRANSMITTED INFORMATION. 10
7.0 WAVENET SYSTEM 3065 NETWORK COMPONENTS. 11
7.1 PCs _____ Fehler! Textmarke nicht definiert.
7.2 Router nodes (general) _____ 12
7.3 Router nodes (special variants) _____ 12
7.4 Repeater nodes _____ 13
7.5 Router nodes _____ 14
7.6 Central nodes _____ 18
7.7 LockNode with RS485 interface _____ 18
7.8 Backbone cabling for router / repeater node _____ 20
7.9 Connection specification for wired LockNode (WN.LN.C) _____ 20
7.10 LockNodes _____ 21
8.0 NETWORK STRUCTURE WITH LSM. 24

9.0 SECURITY. 26
9.1 Secure communication between WaveNet nodes _____ 26
9.2 Automatic checking of individual system components _____ 26
9.3 Alarms _____ 26
10.0 BATTERY WARNING. 27
11.0 NETWORK ‘N’ / ‘W’. 27
12.0 REPLACING LOCKNODE BATTERIES. 27
13.0 INSTALLATION OF WAVENET LOCKNODES. 28
14.0 DISPLAY OF OPERATING STATUSES AND LED DISPLAYS. . 29
14.1 WN.RN.(XX), WN.LN.C _____ 29
14.2 WN.RN.R, WN.CN.(X)R, WN.RN.ER _____ 29
14.3 Node defect (through self-test) _____ 29
14.4 WN.RN.(X)C, WN.CN.(X)C: Master _____ 29
14.5 WN.RN.C(X), WN.LN.C: Slave _____ 29
14.6 WN.LN _____ 30
14.7 WN.RN.CC _____ 30
14.8 WN.CN.U(X) _____ 30
14.9 WN.RP.CC _____ 30
15.0 TECHNICAL DATA. 31
15.1 WaveNet plug-in power supplies _____ 31
15.2 WaveNet central node, RS232 connecting cable _____ 31
15.3 WaveNet central node, RS232 / RS 485 interface _____ 31
15.4 WaveNet central node, USB / RS485 interface _____ 32
15.5 WaveNet central node, RS232 / 868 MHz interface _____ 32
15.6 WaveNet central node, USB / 868 MHz interface _____ 33
15.7 WaveNet router node for segment expansion RS485 _____ 33
15.8 WaveNet router node 868 MHz _____ 34
15.9 WaveNet repeater _____ 34
15.10 WaveNet router node as RS485/868 MHz converter _____ 35
15.11 WaveNet router node as 868 MHz/RS485 converter _____ 35
15.12 WaveNet router node as Ethernet/RS485 converter _____ 36

15.13 WaveNet router node as Ethernet/868 MHz converter _____ 36
15.14 WaveNet router node as WLAN/RS485 converter _____ 37
15.15 WaveNet router node as WLAN/868 MHz converter _____ 37
15.16 WaveNet LockNode _____ 38

© Copyright SimonsVoss Technologies AG
All rights reserved

Note: SimonsVoss Technologies AG reserves the rights to make modifications to the product without notice. Consequently descriptions and representations in this documentation may vary from the most recent product and software versions. As a general principle, the original German version shall apply in the event of any doubt. Subject to errors and misspellings.

1.0 INTRODUCTION.

In the text that follows, the components of the System 3060 (locking cylinders, Smart Relays, shunt lock) are always referred to as lock(s) and door(s). Unless explicitly stated otherwise, the information given applies to all other components of the System 3060.

Up to a certain system size, or for customers with a small number of doors, it is advisable to program the System 3060 with a laptop and SmartCD, as this generally means that fewer changes have to be made to the lock configuration.

For medium-sized or larger systems where lost keys, authorisation for new transponders and organisational changes are more frequent, it is advisable to update and maintain the locking system over the network. However, not all doors necessarily need to be networked. The entire system can be configured for combined operation (networking / stand-alone).

In a networked system, not only can all maintenance and programming tasks be performed on a central PC, the current status of the entire network can be interrogated. You can query lock and door statuses such as Door open – Door closed, Door unlocked – Door locked, Battery warning and Access list from a central point. This allows you to respond directly to an event from a central point.

WaveNet is a simple-to-install ‘plug and play’ network for use in building automation. Because it is installed with no wires, it is particularly suitable for online administration and management of the SimonsVoss digital locking and organisation system 3060 in existing buildings; it can however also be used in new buildings (e.g. in flexible-use areas).

Data transfer within a WaveNet network depends heavily on the transmission medium. Data can be transmitted via RS485 interfaces, Ethernet interfaces (TCP/IP), USB interfaces, RS232 interfaces, radio interfaces (868 MHz) and also WLAN.

In summary, networking allows the entire access control system to be configured and monitored from a central PC. This enables the user to respond immediately to critical situations.

We would recommend that you take advantage of the WaveNet training offered at SimonsVoss or WaveNet project planning with a SimonsVoss service technician.

2.0 NOMENCLATURE.

WN→ WaveNet

LN → LockNode

RN → Router Node

RP → Repeater Node

CN → Central Node

S → Serial (RS232)

R → Radio (868 MHz)

C → Cable (RS485)

U → USB

E → Ethernet (TCP/IP)

W → WLAN

X → Placeholder for user's choice of transmission medium

3.0 TRANSMISSION MEDIA.

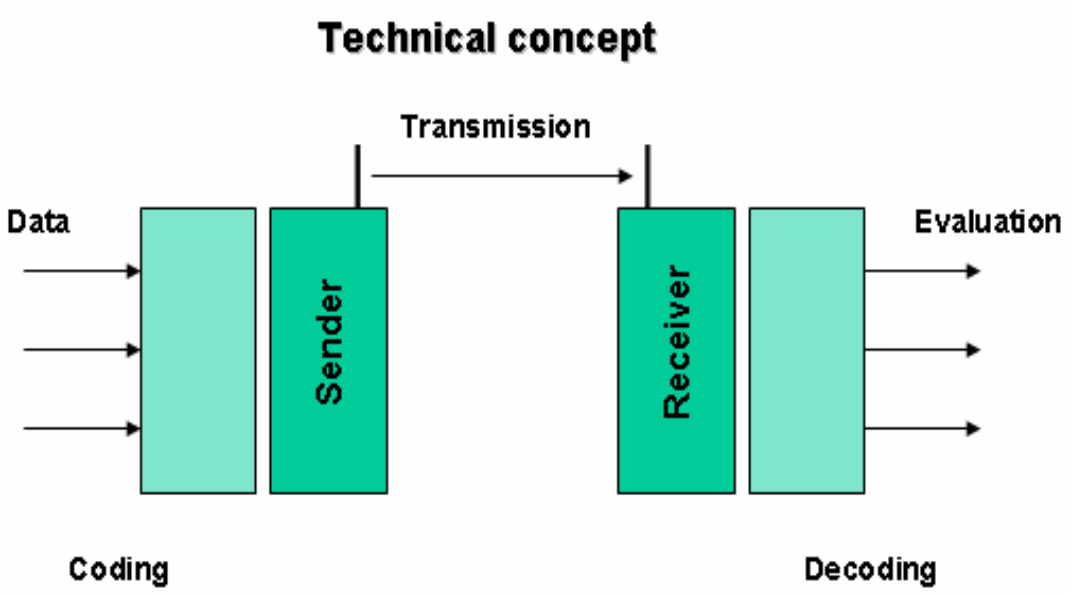
WaveNet supports the following transmission media for the transfer of data within the system:

- RS485 bus cabling for connecting individual WaveNet routers and repeaters as network backbone (cable type: CAT 5, screened, max. cable length 900 m). **WN.RN.(X)C, WN.RN.C(X), WN.RP.CC**, **WN.CN.(X)C**
- RS485 bus cabling for connecting individual WaveNet LockNodes as wired WaveNet. **WN.LN.C**
- Internet or Intranet via TCP/IP for data transfer within an Ethernet network (10/100 Base T) or WLAN from various WaveNet networks. **WN.RN.EC, WN.RN.ER, WN.RN.WC, WN.RN.WR**
- USB, for data transfer between a PC and the WaveNet central node. **WN.CN.UC, WN.CN.UR** (cable length 1.5 m)
- RS232, for data transfer between a PC and the WaveNet central node. **WN.CN.SC, WN.CN.SR** (maximum cable length 2 m)
- 868 MHz radio (radio range approx. 20 - 40 m, depending on building structure) **WN.RN.(X)R, WN.RN.R(X), WN.CN.(X)R, WN.LN**
- B-field 25 kHz (radio range approx. 30 cm), for data transfer between the WaveNet LockNode and the SimonsVoss lock (e.g. locking cylinder, Smart Relay, etc.)

4.0 USABLE RADIO BANDS.

The modern radio technologies used in security technology should not be confused with the kind of radio system found in your car or in future in-home communication.
Radio transmission in access control systems must satisfy the necessary security standards.

In 2000 a special SRD (short range device) band in the 868 MHz range was made available for this type of application. The advantage of this SRD band is that there is a clear set of rules governing the usage of sub-bands per time unit. This means that a radio device (e.g. router node) that uses a frequency channel in the 868 MHz range is only allowed to transmit for 36 seconds every hour. These rules are set out in the duty cycle regulations.
This pre-empts permanent users and therefore sources of interference with regard to secure radio transmission, such as wireless headsets and amateur radio operators. There are also ranges reserved exclusively for security applications.
Basic information and specifications about the system technology, such as size of components, minimum ranges, battery lifetime etc., provide a sufficiently secure means of transmission for the use of WaveNet in the 868 MHz range. In the US the 915 MHz band is used, and this is also available from SimonsVoss.



5.0 WHAT ARE THE BASIC INFLUENCING FACTORS?

Regardless of the transmission procedure, radio transmission is subject to various environmental factors which can disrupt or hinder transmission. Device characteristics can also have an effect on range.

What does range depend on?

- Transmission power
- Antennas
- Sensitivity of receiver
- Environment (air humidity, temperature, external interference)
- Installation site
- Frequency

Structural environment (walls, ceilings etc.)

Transmission range can also be limited by obstacles. The table below provides approximate values:

Material	**Energy penetration**
Wood, plaster, plasterboard	90-100 %
Brick, chipboard	65-95 %
Reinforced concrete (transmitter on metal)	10-70 %
Metal, metal lattice, aluminium laminate, under floor heating	0-10 %

6.0 SECURITY OF TRANSMITTED INFORMATION.

The security of information transmitted by radio in WaveNet depends on:

- radio transmission security in relation to data telegram management
- potential sources of interference
- deliberate disruption, i.e. manipulation or sabotage
- intelligent measures taken to avoid interference and find alternative routes

The speed of data transfer / transmission, like the loss of a percentage proportion of information, may also depend on various influencing factors.

These factors may include:

- high data traffic within WaveNet
- external interference in WaveNet's radio range
- power failure in WaveNet's segment areas
- transmission failure or disruption in an external network (e.g. LAN)

7.0 WAVENET SYSTEM 3065 NETWORK COMPONENTS.

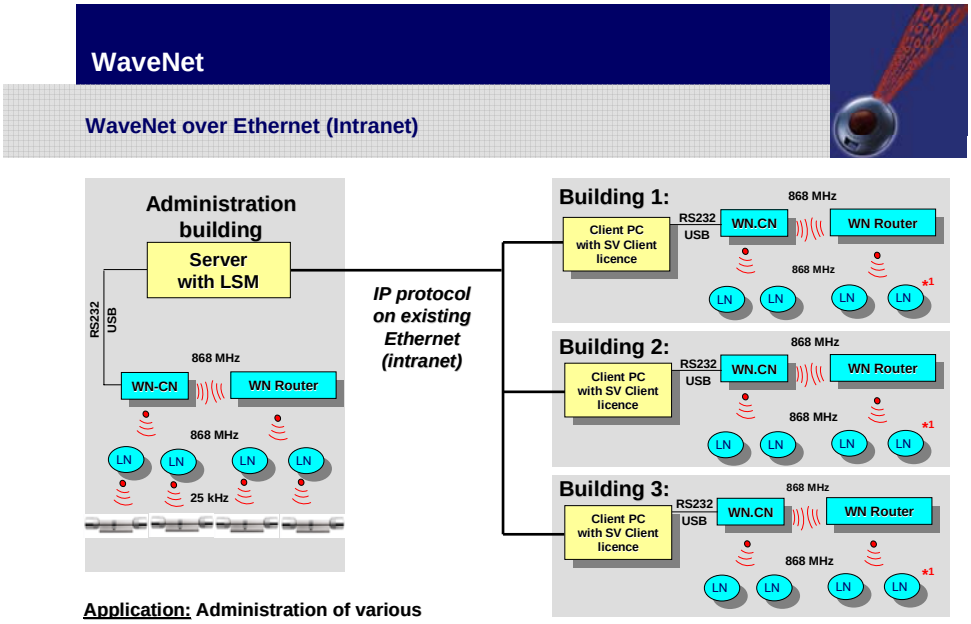
WaveNet network components essentially have two mutually independent interfaces. This makes it possible to connect two different network segments via the WaveNet network components. **WN.CN.(XX), WN.RN.(XX)**

Definition: Network segments are characterised firstly by a certain transmission medium (e.g. RS485 cable, Ethernet (TCP/IP), USB, RS232 cable, 868 MHz radio, WLAN) and secondly by an individual input and output segment address (GID = Group ID → slave or master address)

The following SimonsVoss WaveNet network components are available:

PCs can be integrated into WaveNet using special communication node software (CommNode):

- between the user interface and RS232 interface or
- between the user interface and TCP/IP (Internet, Intranet) or
- between the user interface and USB interface



Application: Administration of various Buildings/Halls (at a single site) over an existing Ethernet (Intranet)

*1: The LN communicates at 25 kHz with the corresponding assigned locking (see administration building)

SimonsVoss technologies

7.1 Router nodes (general)

WaveNet router nodes connect two different network segments which use either the same transmission medium (e.g. RS485-RS485) or different transmission media (e.g. RS485 cable/radio 868 MHz, Ethernet/RS485 or radio 868 MHz, WLAN/RS485 or radio 868MHz).
The WaveNet router node also filters the data flows from the segments so that the only data forwarded to the segment downstream of the WaveNet router node is the data to be processed in this same segment. All other data is blocked from the downstream segment by the WaveNet router node.
At present, WaveNet router nodes can connect the following transmission interfaces between segments: RS485 CAT 5 cable, Ethernet TCP/IP, USB, RS232 cable, radio 868 MHz, WLAN.

7.2 Router nodes (special variants)

WaveNet central nodes are router nodes that can interconnect

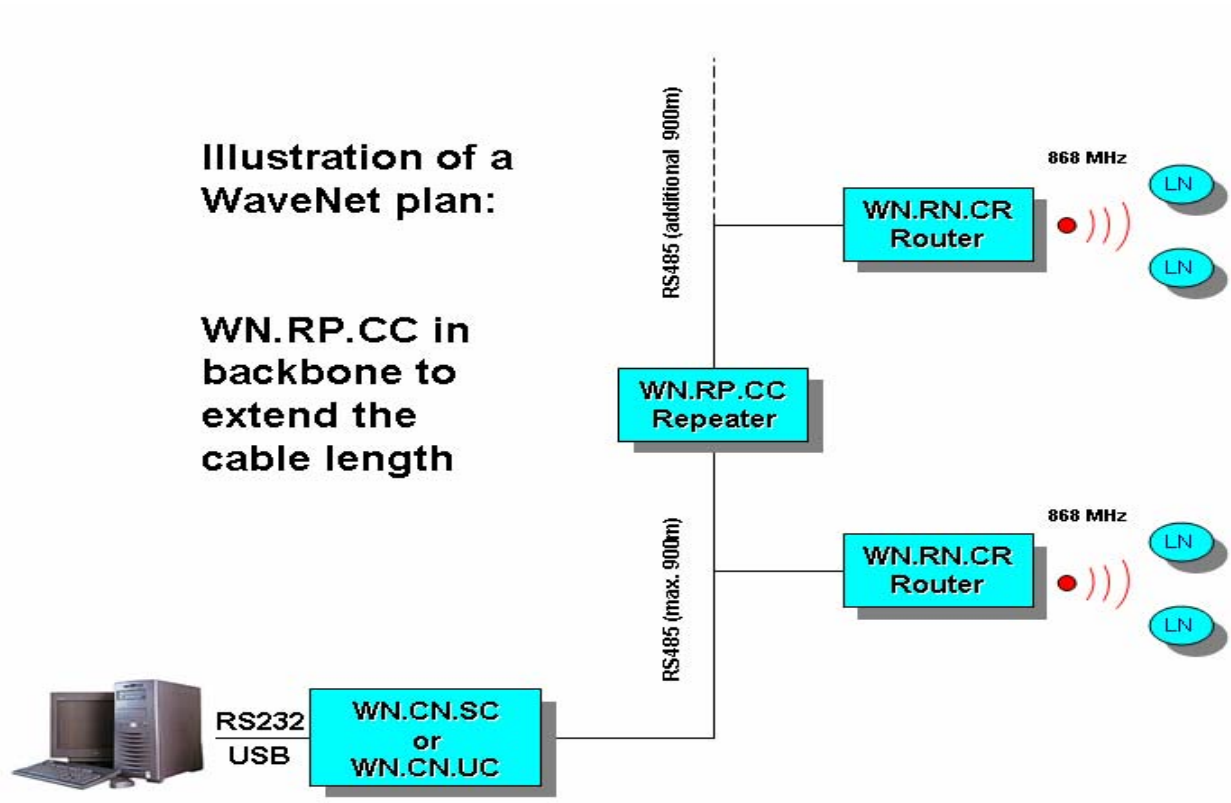
- between PC (RS232 interface) and radio 868 MHz or
- between PC (RS232 interface) and CAT 5 cabling (RS485) or
- between PC (USB interface) and radio 868 MHz or
- between PC (USB interface) and CAT 5 cabling (RS485).

WaveNet router nodes interconnect

- between Ethernet (TCP/IP) and radio 868 MHz or
- between Ethernet (TCP/IP) and CAT 5 cabling (RS485) or
- between WLAN and radio 868 MHz or
- between WLAN and CAT 5 cabling (RS485)

7.3 Repeater nodes

WaveNet repeater nodes are repeaters that can be used within one segment to extend the range (wiring length). In other words, if the cable laid in the network exceeds the specified length (up to 900 m), it can be extended using the WaveNet repeater node **(WN.RP.CC)** in accordance with the system specifications.



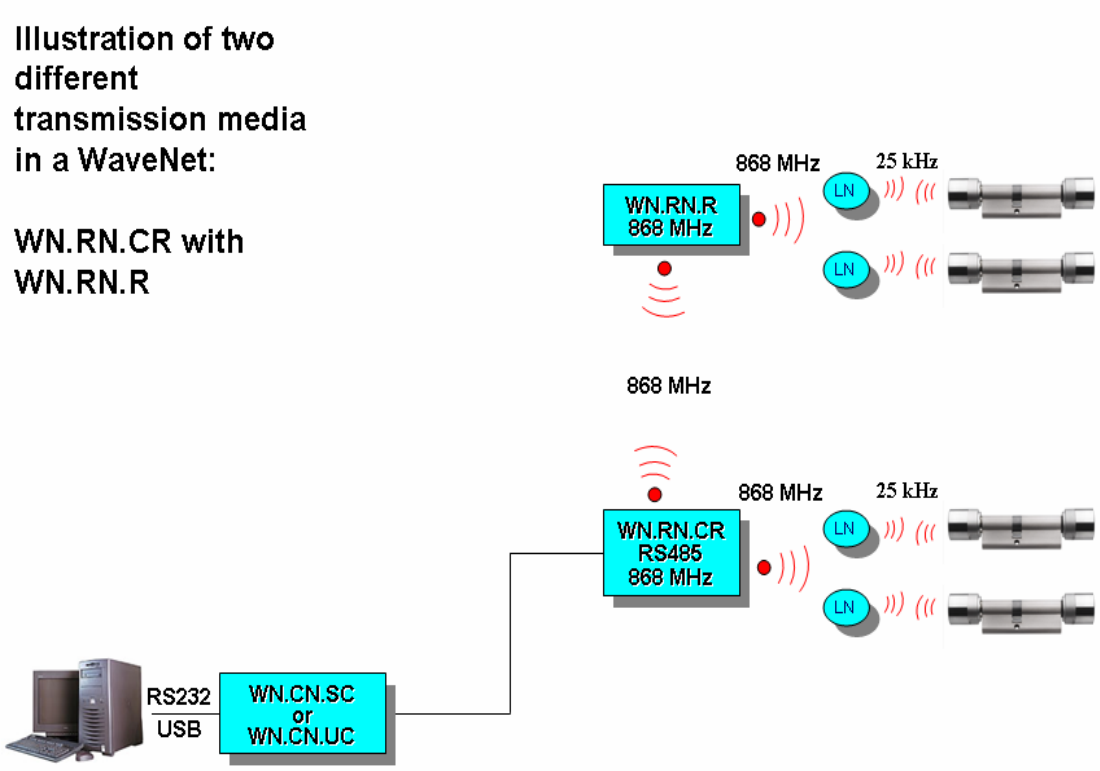
7.4 Router nodes

WaveNet router nodes as converters from radio (868 MHz) to cable (RS485) or from cable to radio. **WN.RN.RC** or **WN.RN.CR**

- The user is free to select the transmission medium depending on the building structure / installation situation

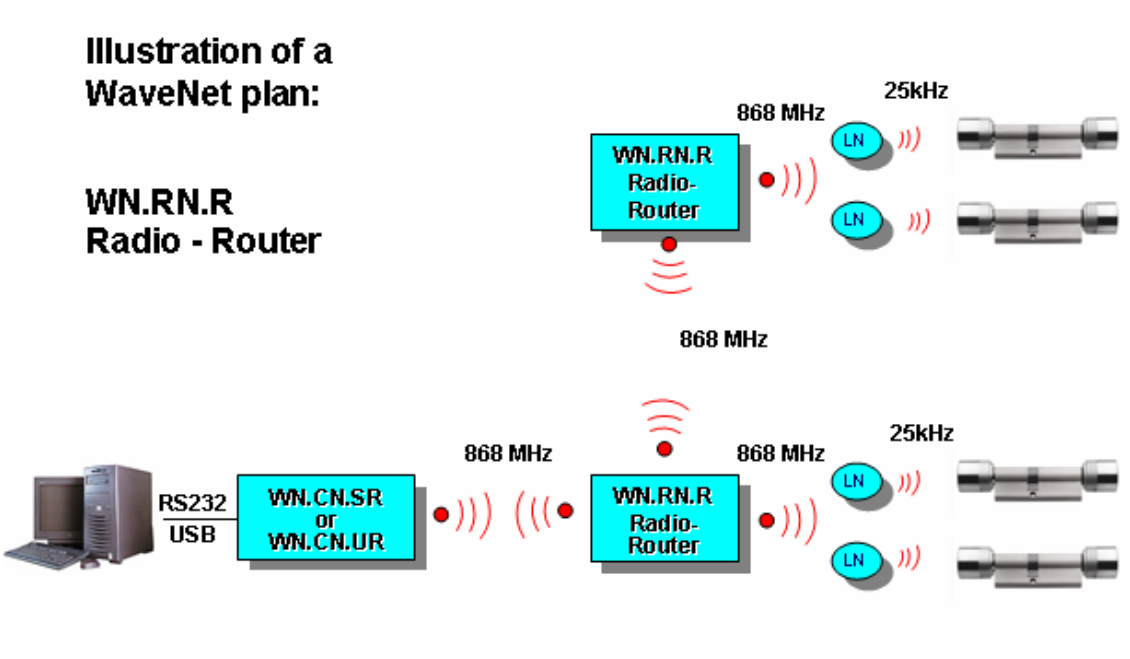
Illustration of two different transmission media in a WaveNet:

WN.RN.CR with WN.RN.R



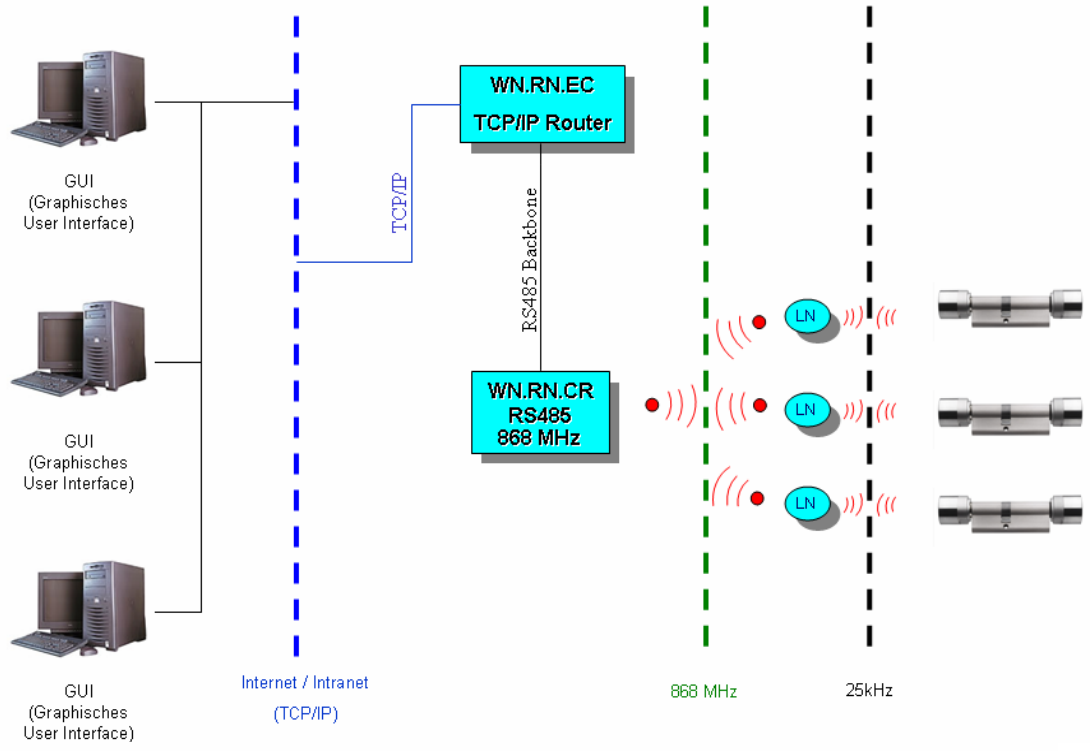
WaveNet router nodes can be used

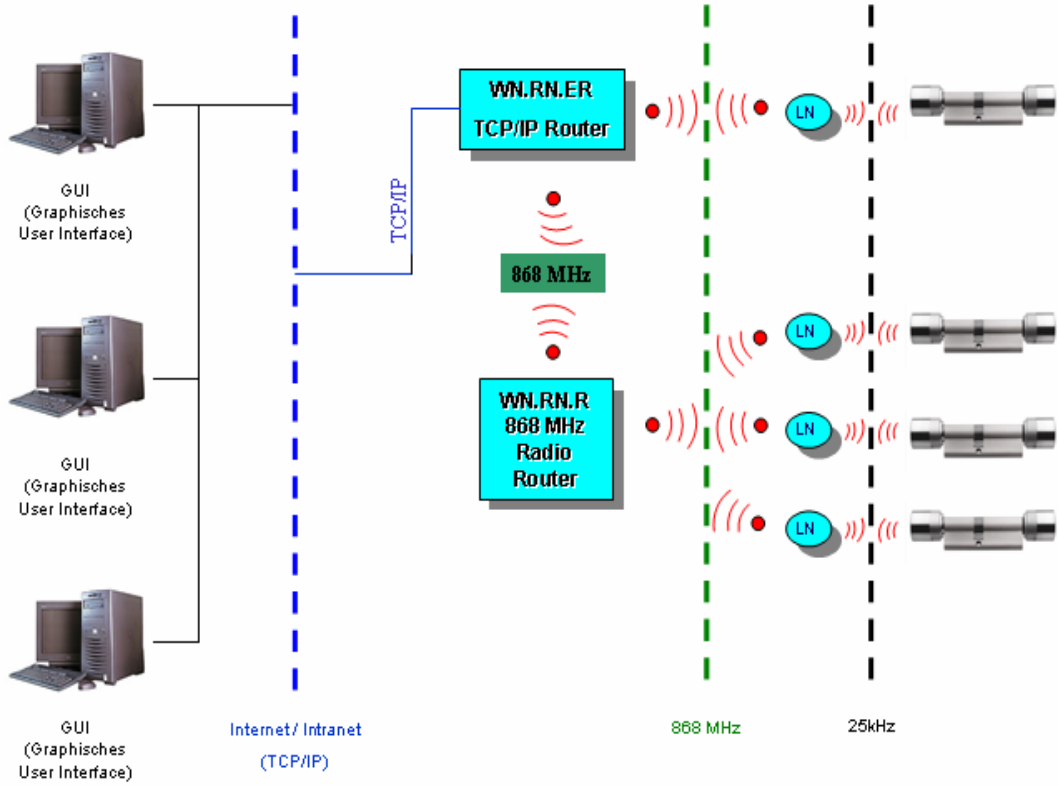
- If you require a radio range to a LockNode that exceeds the radio range of the WaveNet router node (the radio signal is sent from one WaveNet router node (868 MHz) to another WaveNet router node and then to the LockNode (LN)). **WN.RN.R**



WaveNet router nodes can be used

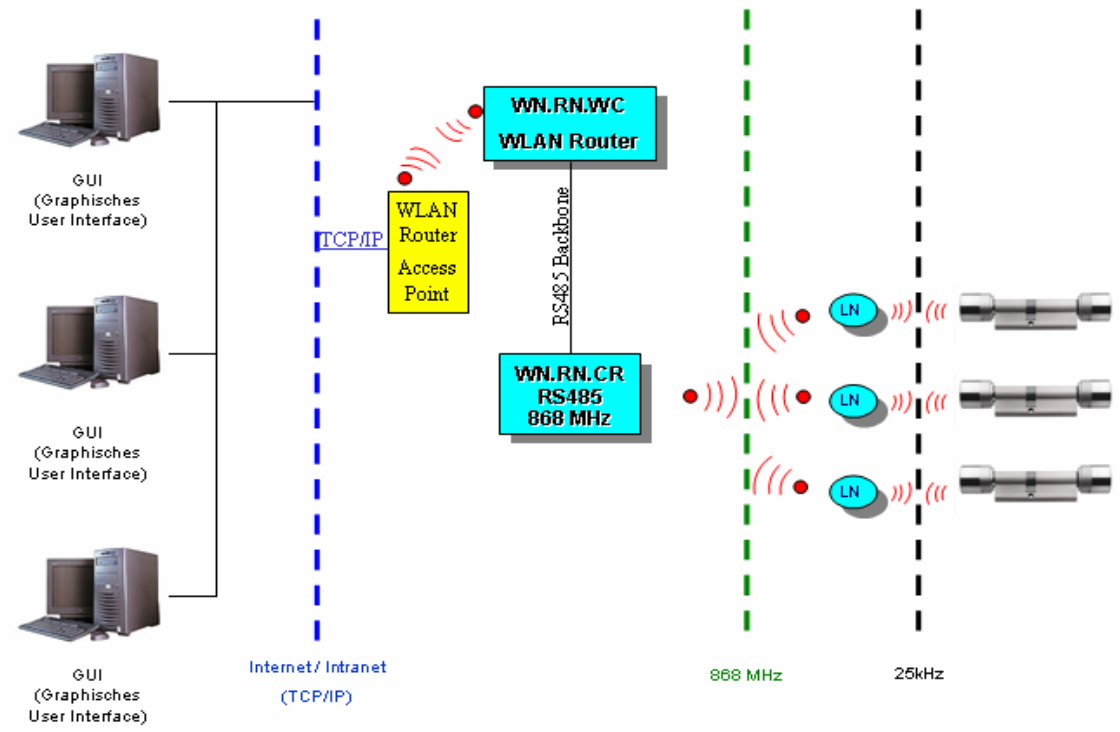
- If there is a computer network (LAN) or Internet/Intranet installed at the customer's premises. Any transmission media may be selected. **WN.RN.E(X)**

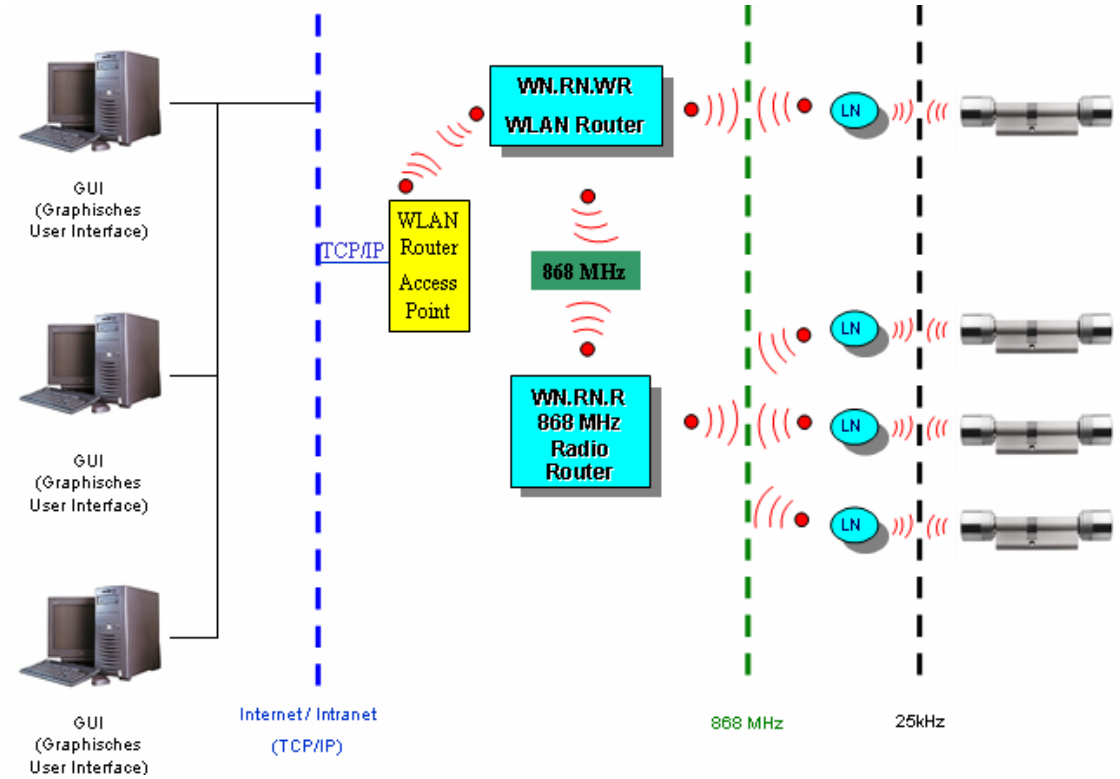




WaveNet router nodes can be used

- If there is a computer network (WLAN) or Internet/Intranet installed at the customer's premises. Any transmission media may be selected. **WN.RN.W(X)**

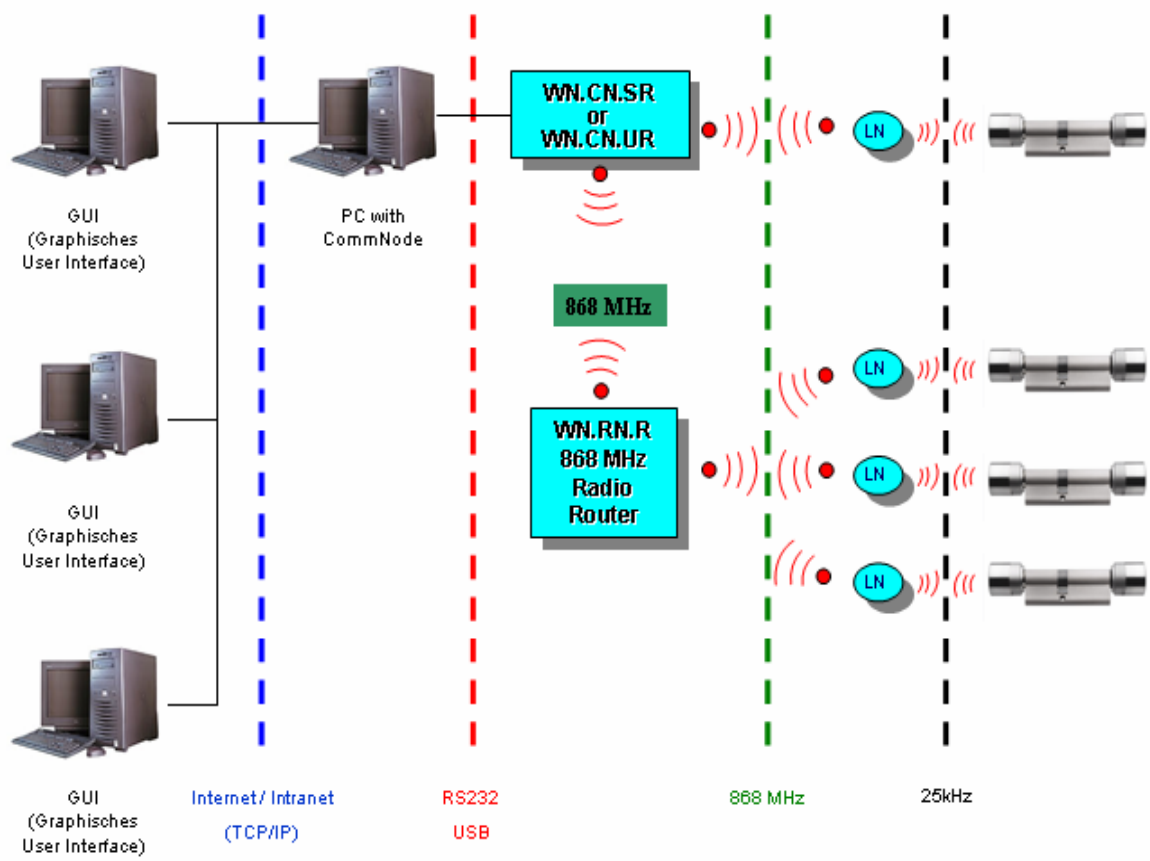




7.5 Central nodes

WaveNet central nodes can be used

- If there is a computer network (LAN) or Internet/Intranet installed at the customer's premises. Any transmission media may be selected. The central nodes **WN.CN.S(X)** or **WN.CN.U(X)** are connected to the PC. Communication node software (CommNode) is installed on this PC. This allows the central node to be addressed from any location (GUI = Graphic User Interface) in the network. A central node can of course also be connected 'locally' to a PC.



7.6 LockNode with RS485 interface

WaveNet LockNodes with integrated RS485 interface allow you to create a 'wired' WaveNet. For the cable type, select CAT 5 or higher. As a connection is provided for an external power supply (max. 24 V DC), the LockNodes are not battery-operated (see 7.9). Up to 250 LockNodes can be administered in each segment. To expand a segment you always need a **WN.RN.CC**. The maximum cable length per segment is 900 m. If the cable length is exceeded, you will need a **WN.RP.CC**. This high-speed repeater serves to forward signals in both directions (up/down link). The repeater does not expand the segment.

Illustration of a „wired“ (RS485) WaveNet plan:

WN.LN.C with Router Node for segment extension in backbone

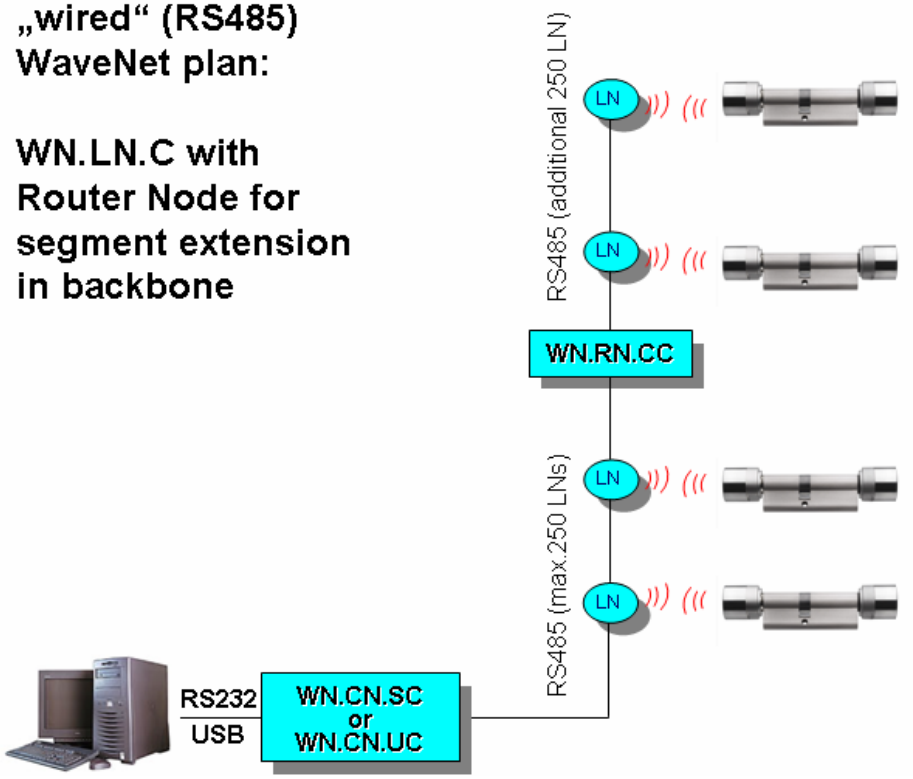
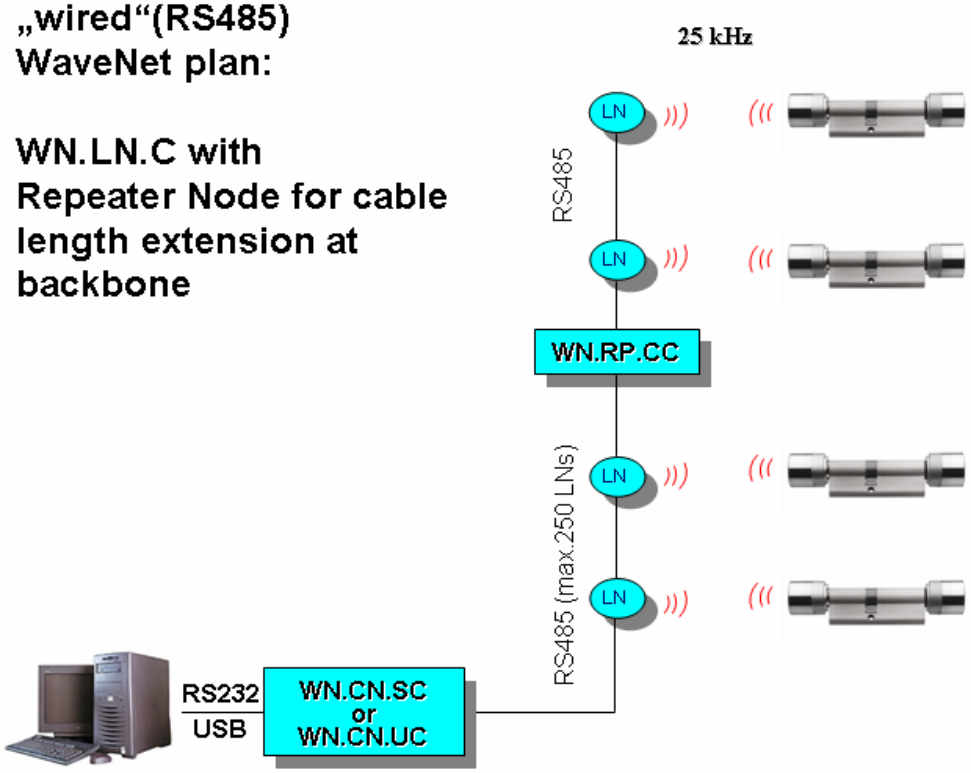


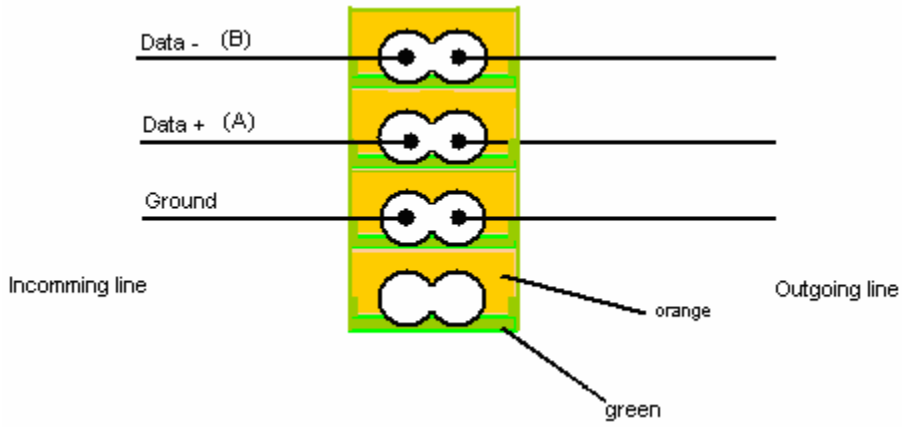
Illustration of „wired“(RS485) WaveNet plan:

WN.LN.C with Repeater Node for cable length extension at backbone

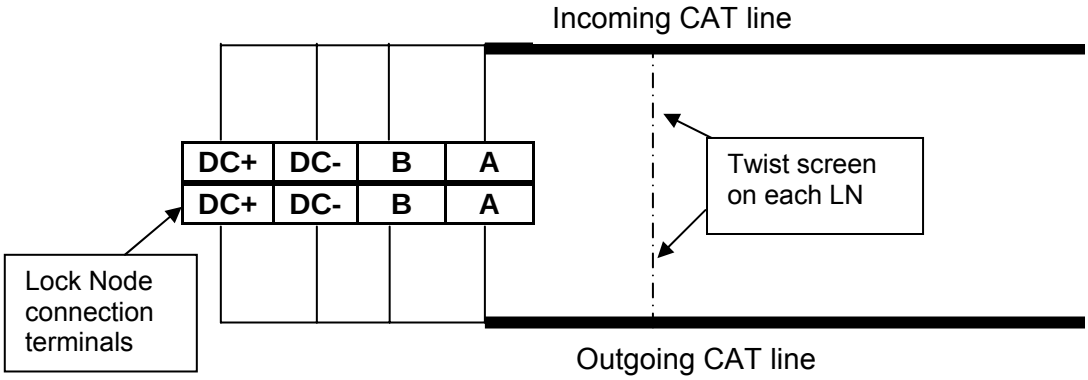


7.7 Backbone cabling for router / repeater node

An RS485 segment (backbone) is wired up using a bus line in the form of a screened standard CAT 5 cable. The bus line consists of two data lines (Data+, Data-) and a ground line (screening).
This bus line is connected to each RS485 module in the WaveNet router for this segment. The RS485 modules are in contact with the bus line via a green and orange 8-pin Phoenix connector, as shown below:



7.8 Connection specification for wired LockNode (WN.LN.C)

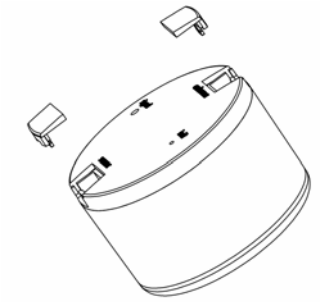


DC: Connection to 6-24V DC power supply, polarity-dependent!
Power consumption of LockNode: 15 mA

A: Connection to data line D+, polarity-dependent!
B: Connection to data line D -, polarity-dependent!

Screening: On each LockNode / router node the screening must be connected through, insulated and in contact with one ground potential (PE)!!!

7.9 LockNodes



Lock Node
with housing

WaveNet LockNodes represent the interface between WaveNet and the locks in the digital locking and organisation system 3060 (e.g. locking cylinders, Smart Relays etc.).

They always have:

- a special B-field interface which enables communication with SimonsVoss locks (e.g. locking cylinders, control units/Smart Relays, furniture locks, etc.)
- a radio interface (868 MHz) to ensure data transmission to the WaveNet nodes (e.g. WaveNet router nodes, WaveNet repeater nodes or WaveNet central nodes) or
- an RS485 interface and connection for an external power supply, for operation in a 'wired WaveNet' **(WN.LN.C)**

WaveNet LockNodes can always be assigned to just one digital lock in the system (e.g. a locking cylinder, Smart Relay or furniture lock, etc.). The distance between the WaveNet LockNode and a digital cylinder / furniture lock must be no more than 30 cm. A minimum distance of 40 cm must be maintained between the LockNode and a Smart Relay. We recommend fitting a cable connection between both components with ***WN.KAB.WIRED-BF***. In this scenario, no minimum gap needs to be observed (with SREL.ADV only).

In a radio network, WaveNet LockNodes are **battery-operated** and can therefore be integrated in the SimonsVoss WaveNet with no wiring whatsoever. This makes the system ideal for later installation in an existing building.

The wired variant of the LockNode **(WN.LN.C)** features connections for the RS485 bus and for the external power supply.
(see 7.9).

To simplify installation as far as possible, the housing of the WaveNet LockNode is designed to be installed in a standard built-in mounting box (60 mm deep, 55 mm in diameter) in accordance with **DIN 49073 Part 1** (e.g. for installation in a light switch panel).

Note: *We recommend installing an empty mounting box. This will physically separate the LockNode from the switch unit. A switch unit, e.g. a dimmer or electronic ballast, can have a negative impact on communication between LockNode and lock*.

In addition, no switching power supplies must be used (e.g. as a power supply for the LockNodes). Distance between switching power supply and LockNode / router node: ≥ 2 m.
With some switch ranges, less space is available owing to the cover attachment.

LockNode inputs / output:

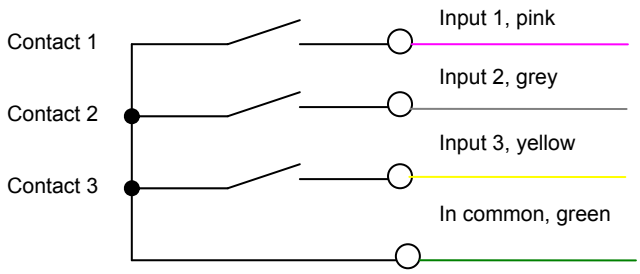
Each WaveNet LockNode also features one output and three inputs, e.g. for door monitoring (except WN.LN.O.I/O).

The three inputs allow up to three external potential-free contacts to be connected. This allows for the central monitoring of door or bolt contacts, for example, but also motion sensors, light barriers etc., over the WaveNet network.

The statuses of connected contacts can be interrogated (polled) from the central computer at any time. Modifications to the contacts (events) can also be reported automatically to the central computer if the LockNode is configured accordingly.

The output forwards signals to external systems such as signal transmitters, heating, lighting etc. The output takes the form of an electronic switch (open drain) that can switch up to 25 V and up to 650 mA.

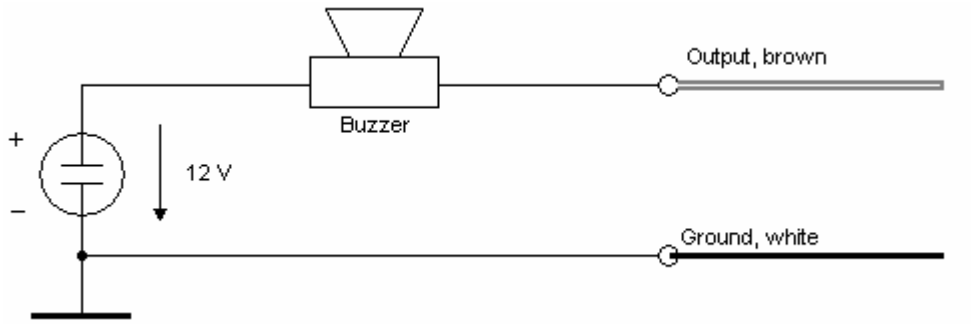
For the optional **activation of I/Os** there is a 6-pin colour-coded cable **(WN.LN.SENSOR.CABLE**) which is connected to the socket labelled ‘sensor’ on the LockNode. For monitoring tasks, up to three potential-free contacts can be connected between the green ‘in common’ line and each of the coloured (pink, grey, yellow) lines (see diagram).



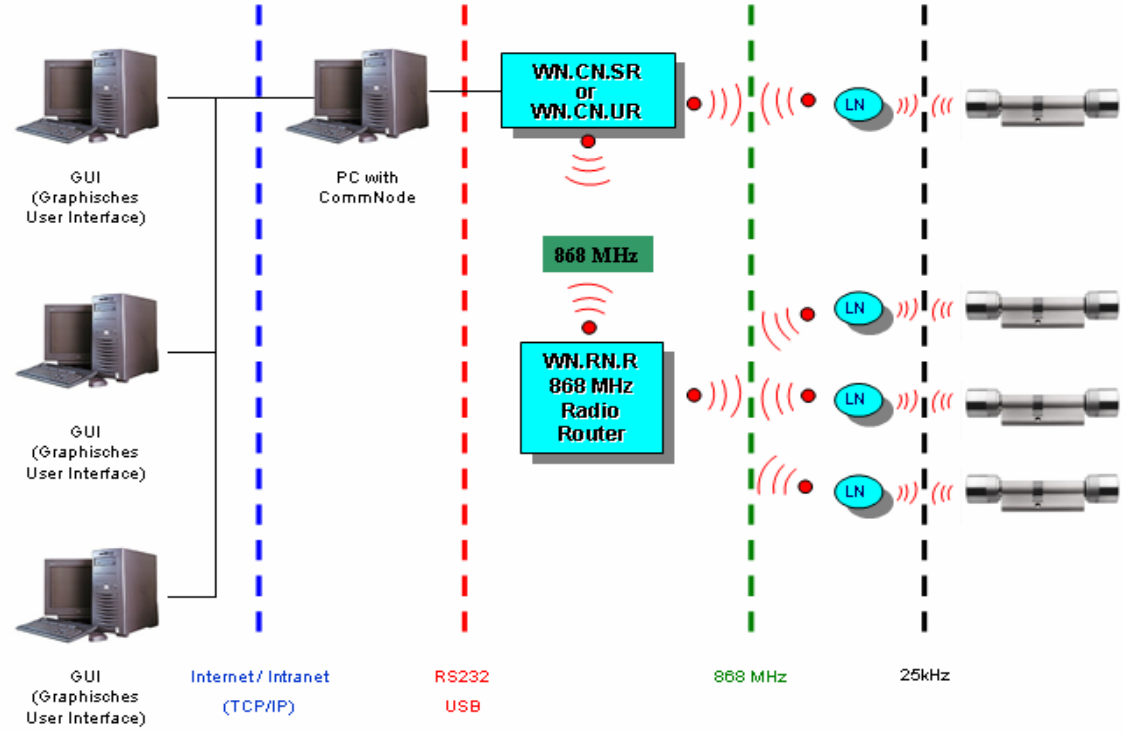
In the LDB or LSM user interface, an open contact has a value of 0 and a closed contact has a value of 1. In the diagram above, for example, if contact 1 is used to monitor a door, an opening door will constitute an event: ‘Input1 transition from 1 to 0’, if contact 1 is closed when the door is closed and open when the door is open.

Internally, the output takes the form of a transistor in open-collector switching. The white and brown cables are available for connecting to external devices (e.g. buzzers). The following applies: Out = brown, ground = white.

Connection example for possible output circuit:



8.0 NETWORK STRUCTURE WITH LSM.



The network structure shown above allows different users with individual rights to access a shared server via the Internet / Intranet using the SimonsVoss WaveNet communication node software (CommNode) and the GUI (Graphic User Interface). This server functions as a communication node and is connected to the WaveNet central node by an RS232 cable or a USB cable.

In the example above, the WaveNet central node connected to the server communicates directly by radio (868 MHz) with a LockNode, which in turn exchanges data by radio (25 kHz) with the digital components (locking cylinders).
In the example shown above, all other LockNodes are outside the radio range of the WaveNet central node and are therefore addressed indirectly through a WaveNet router node.

The above structure can be configured elegantly with the multi-user, multi-client, database-based LSM locking system administration software from SimonsVoss. However, the above example only includes one comm node and therefore only one central node with a local sub-network. In reality, virtually any number of comm nodes can be distributed in the Intranet or Internet. For example, you can set up a ‘branch system’ whereby you can address any number of branches with local central nodes and associated sub-networks over the Intranet / Internet from a central point.

In the LSM, virtually any number of WaveNet Ethernet routers **WN.RN.E(X)** or WaveNet WLAN (Wireless Local Area Network) routers **WN.RN.W(X)** can be integrated in a customer computer network (LAN or WLAN). There is no need to install a backbone (RS485 bus cabling), but it is possible in locations without Ethernet/WLAN.

The **WN.RN.E(X)** is PoE-capable (Power over Ethernet). If you are using PoE so you will need a midspan power supply such as *Phihong PSA 16 U.*
Alternatively, **WN.RN.E(X)** and all **WN.RN.(XX)** configurations can be operated with a plug-in power supply. → WN.POWER.SUPPLY.PPP (not included in delivery).

The file-based LDB locking system administration software from SimonsVoss (which is much simpler to install and easier to operate) also enables direct integration of the transmission medium into the Intranet / Internet. To do this, a WaveNet router node is connected to the customer's LAN and configured using LDB or additional software (Digi Connect) (see manual for WN.RN.E(X)). A maximum of four WaveNet routers can be administered in one LDB, but only one can be activated. → Applies to **WN.RN.E(X)** and **WN.RN.W(X)**

Networks are divided into segments. One WaveNet central node can operate up to 252 segments, and each segment can have up to 250 WaveNet LockNodes / WaveNet router nodes.

Note: If you are working with the LSM software, you can also have a distribution of 2030/30 and 250/250 (segments / LockNodes per segment). During the project planning phase you can decide whether you need more segments or more LockNodes per segment.

9.0 SECURITY.

Since WaveNet records and logs critical data, it must be reliably protected against unauthorised access. This demands high standards of the system in terms of information security and manipulation security.

9.1 Secure communication between WaveNet nodes

Network communication is protected against eavesdropping and data monitoring by sophisticated cryptography.

9.2 Automatic checking of individual system components

Because the individual components can be installed over large areas of a building, the system must automatically recognise malfunctions, manipulations and the opening of a door and report them to the controlling PC.

Important: If you want a door to be fitted with door monitoring it must be equipped with at least a door contact that recognises the opening status.

9.3 Alarms

Alarms are messages requiring an immediate response (e.g. break-in, fire). WaveNet is not intended to replace fire or intruder alarm systems!

10.0 BATTERY WARNING.

If the voltage of the batteries fitted in the LockNode falls below a certain level, communication problems may arise both between the LockNode and the associated lock and between the LockNode and a router node (WaveNet router node, WaveNet central node).

If any such problems arise, the 'N' after the relevant lock will be shown in red (indicating communication fault). If the red 'N' does not turn yellow or blue even after repeating the protocol, check whether the battery needs to be replaced.

11.0 NETWORK 'N' / 'W'.

In the LDB/LSM, locks/doors are labelled with an 'N' / 'W' if they are fitted with a LockNode. 'N's' / 'W's' are shown in the following colours to differentiate between statuses.

Red 'N'/'W':	No connection to LockNode.
Yellow 'N'/'W':	Connection to LockNode but not to lock (door may be open)
Blue 'N'/'W':	Connection to LockNode and to lock

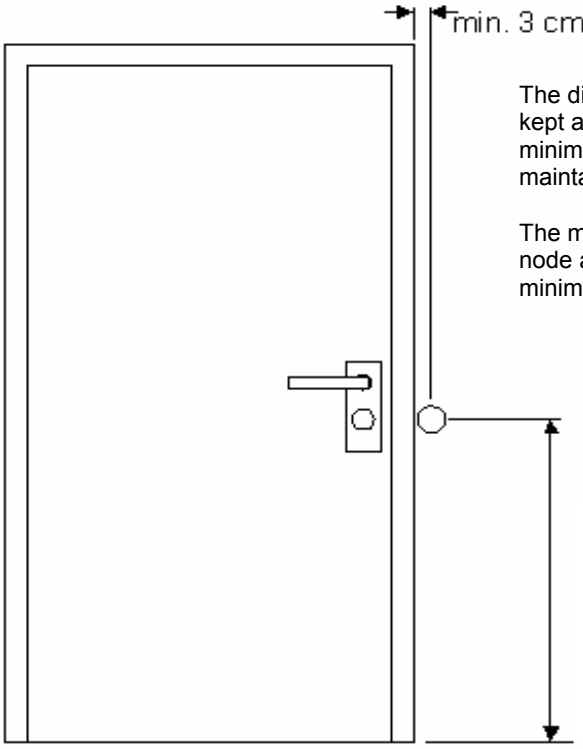
12.0 REPLACING LOCKNODE BATTERIES.

To replace the batteries in the LockNode, you need to remove the LockNode from its installation position (e.g. built-in mounting box) and unscrew the cover on the back.

The position of the two batteries is clearly labelled in the battery compartment. Only use batteries which have been approved by SimonsVoss.

When inserting the new batteries, please observe the LED. Immediately after you insert the first new battery in the empty battery compartment, the LED must flash briefly twice. The node is then ready for operation (power-on reset). If the LED does not light up, please take the battery out again, short-circuit the battery contacts of the LN and re-insert the battery.

13.0 INSTALLATION OF WAVENET LOCKNODES.


min. 3 cm
The distance to the locking cylinder must be kept as short as possible. However, a minimum gap of 3 cm from the frame must be maintained.
The max. distance between WaveNet lock node and locking cylinder is 30 cm. The minimum distance is 10 cm.
The WaveNet lock node should be installed at the height of the locking cylinder. (Preferably install in standard built-in mounting box and light frame with cover).

- The radio ranges of RNs and LNs are generally at their maximum when router nodes are fitted with the antenna aligned vertically, pointing upwards (or downwards). The ‘Init’ button on the LockNode should always point towards the digital cylinder. If the LockNode is installed to the right, next to the cylinder, for example, the SimonsVoss logo will be upside down.

14.0 DISPLAY OF OPERATING STATUSES AND LED DISPLAYS.

14.1 WN.RN.(XX), WN.LN.C

- Power-on reset: 2 x short red flashes
- Link quality between two WN.RN.R by activating button on baseboard:

1/2 flashes of signal LED → Transmission and reception power poor
3/4 flashes of signal LED → Transmission and reception power OK
5/6 flashes of signal LED → Transmission and reception optimal

14.2 WN.RN.R, WN.CN.(X)R, WN.RN.ER

- If the green LED flashes slowly, listening mode is active or
- flashes quickly, communication is present with the LockNode
- Red LED off

14.3 Node defect (through self-test)

- Continuous red light: Hardware defect

14.4 WN.RN.(X)C, WN.CN.(X)C: Master

- Red flicker, green LED off: No segment slave found (cable is defective or no functioning slave)

14.5 WN.RN.C(X), WN.LN.C: Slave

- Red flicker, green LED off: No segment master found (cable is defective or no functioning slave)

For 14.4-5: Flickering of both LEDs means everything is OK.

14.6 WN.LN

- Power-on reset: 2 x short red flashes
- Battery status (after power-on reset):
- 1 x short red flash → Battery fully charged
- 1 x long red flash → Battery critical
- 1 x continuously on > 4 seconds → Battery flat

- Link quality between WN.(X)N.(X)R and LockNode by activating button on LockNode baseboard:

1/2 flashes of signal LED → Transmission and reception power poor
3/4 flashes of signal LED → Transmission and reception power OK
5/6 flashes of signal LED → Transmission and reception optimal

14.7 WN.RN.CC

- Power-on reset: yellow LED on
- Upstream data traffic (towards master): green LED on
- Downstream data traffic (from master): dark green LED on

14.8 WN.CN.U(X)

- USB correctly recognised and power-on reset: yellow LED on
- If the green LED flashes slowly, listening mode is active or
- flashes quickly, communication is present with the LockNode
- Red LED off

14.9 WN.RP.CC

- Voltage present: yellow LED on
- Upstream data traffic: green LED on
- Downstream data traffic: dark green LED on

15.0 TECHNICAL DATA.

15.1 WaveNet plug-in power supplies

Order number	WN.POWER.SUPPLY.PPP
Description	Externally regulated 230V AC / 9V DC / 250 mA Plug-in power supply for WaveNet central node, WaveNet repeater node & WaveNet router node (PPP = Plug Power Pack)

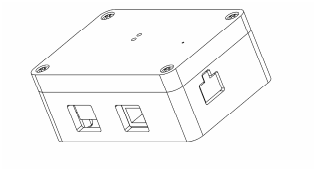
Order number	WN.POWER.SUPPLY.LNC
Description	Externally regulated 230V AC / 24V DC / 1.25A Plug-in power supply only for WN.LN.C, WN.RP.CC, WN.RN.E(X) and WN.RN.W(X) with various network adapters for UK/US/AU

15.2 WaveNet central node, RS232 connecting cable

Order number	WN.CN.RS232.Cable
Description	RS232 connecting cable between PC and WaveNet central node
Length	2 m

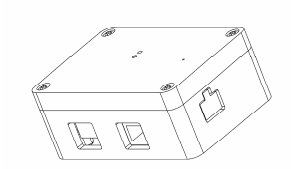
Note: Versions of the housing shown as of 15.3 may vary from the original!

15.3 WaveNet central node, RS232 / RS 485 interface



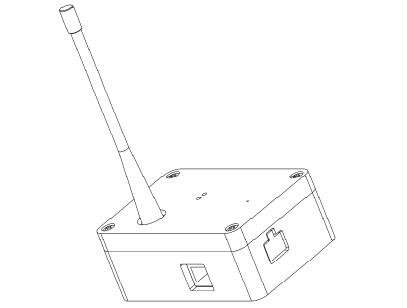
Order number	WN.CN.SC
Description	WaveNet central node for connecting to a PC/server. Central node with integrated RS485 interface for backbone
Dimensions (L*W*H)	100x65x40 mm (applies to all routers without antenna)
Power supply	9V ... 12 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.4 WaveNet central node, USB / RS485 interface



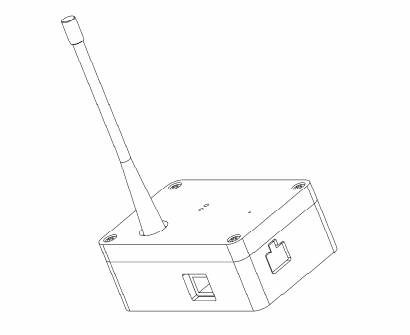
Order number	WN.CN.UC
Description	WaveNet central node for connecting to a PC/server. Central node with integrated RS485 interface for backbone
Dimensions (L*W*H)	100x65x40 mm (applies to all routers without antenna)
Power supply	From USB port
Output	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.5 WaveNet central node, RS232 / 868 MHz interface



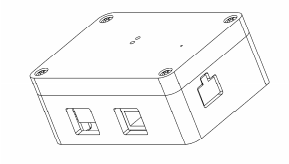
Order number	WN.CN.SR
Description	WaveNet central node with 868 MHz radio interface and external antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)
Power supply	9V ... 12 V DC regulated plug-in power supply
Output	Min. 3 VA (250 mA with continuous load)
For all routers with radio module:	
Maximum transmission power	5 dBm (3.16 mW) at antenna socket
Sensitivity	-90 dBm at 19.2 kBaud
Frequency band	868 MHz
Power consumption in receiver mode	12 mA at 9 V

15.6 WaveNet central node, USB / 868 MHz interface



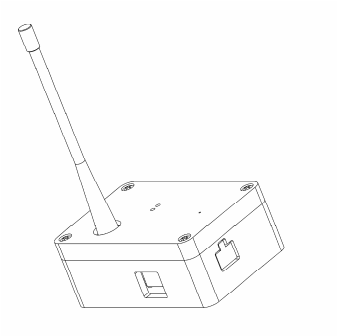
Order number	WN.CN.UR
Description	WaveNet central node with 868 MHz radio interface and external antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)
Power supply	From USB port
Output	Min. 3 VA (250 mA with continuous load)
For all routers with radio module:	
Maximum transmission power	5 dBm (3.16 mW) at antenna socket
Sensitivity	-90 dBm at 19.2 kBaud
Frequency band	868 MHz
Power consumption in receiver mode	12 mA at 9 V

15.7 WaveNet router node for segment expansion RS485



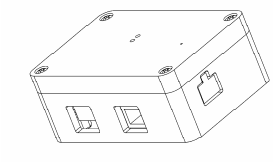
Order number	WN.RN.CC
Description	WaveNet router node as RS485 router with two RS485 interfaces for segment expansion incl. connecting terminal for external plug-in power supply
Dimensions (L*W*H)	100 x 65 x 40 mm
Power supply	9V ... 12 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.8 WaveNet router node 868 MHz



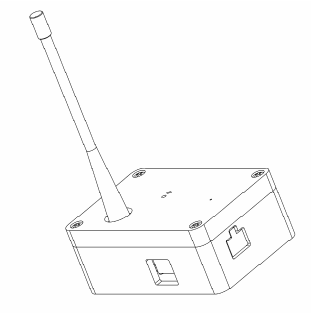
Order number	WN.RN.R
Description	WaveNet router node with 868 MHz radio module. Incl. connecting terminals for external plug-in power supply and external transmission and receiver antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)
Frequency band	868 MHz
Power supply	9V ... 12 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.9 WaveNet repeater



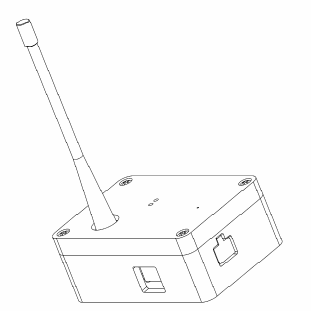
Order number	WN.RP.CC
Description	WaveNet RS485 repeater with two RS485 interfaces to extend line length incl. connecting terminal for external plug-in power supply
Dimensions (L*W*H)	100 x 65 x 40 mm
Power supply	9V ... 40 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.10 WaveNet router node as RS485/868 MHz converter



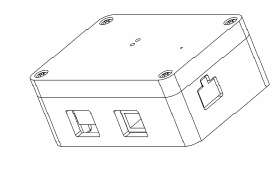
Order number	WN.RN.CR
Description	WaveNet router node as converter between RS 485 interface and 868 MHz interface for using router node as backbone, incl. connecting terminals for external plug-in power supply and external transmission and receiver antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)
Frequency band	868 MHz
Power supply	9V ... 12 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.11 WaveNet router node as 868 MHz/RS485 converter



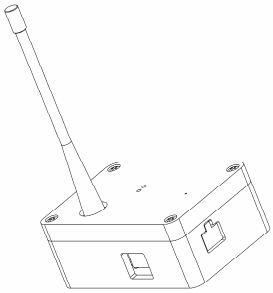
Order number	WN.RN.RC
Description	WaveNet router node as converter between 868 MHz and RS 485 interface for using router node as backbone, incl. connecting terminals for external plug-in power supply and external transmission and receiver antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)
Power supply	9V ... 12 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.12 WaveNet router node as Ethernet/RS485 converter



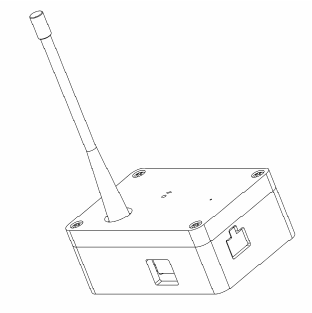
Order number	WN.RN.EC
Description	WaveNet router node as converter between Ethernet interface (TCP/IP) and RS 485 interface for using router node as backbone, incl. connecting terminals for external plug-in power supply
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)
Frequency band	868 MHz
Power supply	9V ...48 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.13 WaveNet router node as Ethernet/868 MHz converter



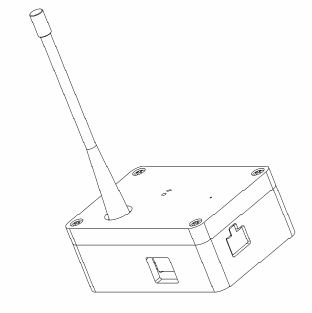
Order number	WN.RN.ER
Description	WaveNet router node as converter between Ethernet interface (TCP/IP) and 868 MHz interface. Incl. connecting terminals for external plug-in power supply and external transmission and receiver antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)
Frequency band	868 MHz
Power supply	9V ... 48 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.14 WaveNet router node as WLAN/RS485 converter



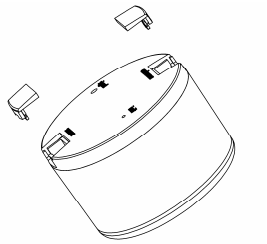
Order number	WN.RN.WC
Description	WaveNet router node as converter between WLAN interface (TCP/IP) and RS 485 interface for using router node as backbone, incl. connecting terminals for external plug-in power supply
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with antenna)
Frequency band	868 MHz
Power supply	9V ... 48V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.15 WaveNet router node as WLAN/868 MHz converter



Order number	WN.RN.WR
Description	WaveNet router node as converter between WLAN interface (TCP/IP) and 868 MHz interface. Incl. connecting terminals for external plug-in power supply and external transmission and receiver antenna
Dimensions (L*W*H)	100 x 65 x 40 mm or 100 x 65 x 130 mm (with 2x antenna)
Frequency band	868 MHz
Power supply	9V ... 48 V DC regulated plug-in power supply
Output (for all routers)	Min. 3 VA (250 mA with continuous load*) * - Peak current with termination of both ends in backbone

15.16 WaveNet LockNode



Order number	**WN.LN**
Description	Battery-operated WaveNet LockNode (Node for PC networking of digital components) with 3 inputs and 1 output
Dimensions (H x ∅)	37 mm x 53 mm
Power supply	2x CR2/3AA batteries, lithium 3.6 V Tadiran, SL761
Power consumption	Radio transmit: 32 mA; radio receive: 18 mA; Power consumption with no data traffic: approx. 20 µA Note: depends on data traffic and HF interference density
Maximum transmission power	approx. 1 mW
Sensitivity	-95 dBm
Frequency band	868 MHz
Input (3x)	Potential-free (Current pulse approx. 35 µA for 1ms every 0.5 sec)
Output (open drain)	Maximum switching voltage: 25 V DC Maximum inrush current: 2 A Continuous current: 650 mA Internal resistance (AN): 0.5 Ω
Battery life	approx. 6 years
Order number	**WN.LN.O.I/O**
Description	Battery-operated WaveNet LockNode (node for PC networking of digital components) without inputs and output
Dimensions (H x ∅)	37 mm x 53 mm
Power supply	2x CR2/3AA batteries, lithium 3.6 V Tadiran, SL761
Power consumption	Radio transmit: 32 mA; radio receive: 18 mA; Power consumption with no data traffic: approx. 20 µA Note: depends on data traffic and HF interference density
Maximum transmission power	approx. 1 mW
Sensitivity	-95 dBm
Frequency band	868 MHz
Battery life	approx. 6 years

Order number	**WN.LN.C**
Description	WaveNet LockNode with RS485 interface for use in 'wired' WaveNet. (Node for PC networking of digital components) with 3 inputs and 1 output
Dimensions (H x ∅)	37 mm x 53 mm
Power supply	Connecting terminals for external power supply 6-24 V DC
Power consumption	See below → Power supply unit rating Power consumption with no data traffic: approx. 20 µA
Maximum transmission power	approx. 1 mW
Sensitivity	-95 dBm
Frequency band	868 MHz
Input (3x) N	Potential-free (Current pulse approx. 35 µA for 1ms every 0.5 sec)
Output (open drain)	Maximum switching voltage: 25 V DC Maximum inrush current: 2 A Continuous current: 650 mA Internal resistance (AN): 0.5 Ω

Note power supply unit rating for WN.LN.C:
An arithmetic value of 15 mA can be estimated for each LockNode.
15 mA (0.015 A) x number of LockNodes = total current → see 15.1

LON – Network 3065

State of: September 2006

SimonsVoss technologies

LON – Network 3065

Content

1.0 Introduction ____ 4
1.1 General Information ____ 5
1.2 Connection to LPI-10 ____
(Version: Open PCB With External Plug-in Power Supply) ____ 6
1.3 Connection to LPI-10 Compact ____ 6
2.0 The Software ____ 7
3.0 Central Node ____ 8
3.1 Method of Operation ____ 8
4.0 Lock Node ____ 9
4.1 Method of Operation ____ 9
4.2 Assembly Instructions ____ 9
4.3 Antenna Extender ____ 10
4.4 LockNode Inputs and Outputs ____ 12
5.0 LPI-10 ____ 13
5.1 General Warnings ____ 13
5.1.1 Risk of Electric Shock ____ 13
5.2 LPI-10 ____ 13
5.2.1 Method of Operation ____ 13
5.2.2 Assembly Instructions ____ 14
5.3 LPI-10 Compact (Version: compact construction with 230V ____
power supply from the customer) ____ 15
5.3.1 Installation ____ 15
5.3.2 Method of Operation ____ 16
5.3.3 Assembly Instructions ____ 16
6.0 Router ____ 17
6.1 Method of Operation ____ 17
6.2 Assembly Instructions ____ 18
6.3 Installation Example ____ 19

Content

7.0 Repeater 20
7.1 Method of Operation 20
7.2 Assembly Instructions 20
8.0 Terminators 20
9.0 Network Cable 21
9.1 General Information 21
9.2 Cable Laying 21
9.3 Cable Types 21
9.4 Bus-Shaped Cabling (Example) 22
9.5 Star-Shaped Cabling (Example) 22
10.0 Planning Examples 24
10.1 Connecting External Buildings via Twisted Pair, Modem & TCP/IP 24
10.2 Network via Modem 25
10.3 Network via Ethernet 25
11.0 Security 26
11.1 Secure Communication Between the Network Nodes 26
11.2 Automatic Tests of Separate System Components 26
11.3 Alarms 26
12.0 Answers to the Most Common Questions Regarding the Network 27
13.0 Data sheet 29

1.0 Introduction

In the following, we always speak of locking(s) and doors as the System 3060 components (locking cylinder, control unit, Smart Relay, shuntlock). Unless otherwise expressly mentioned, however, this information is valid for all other System 3060 components.

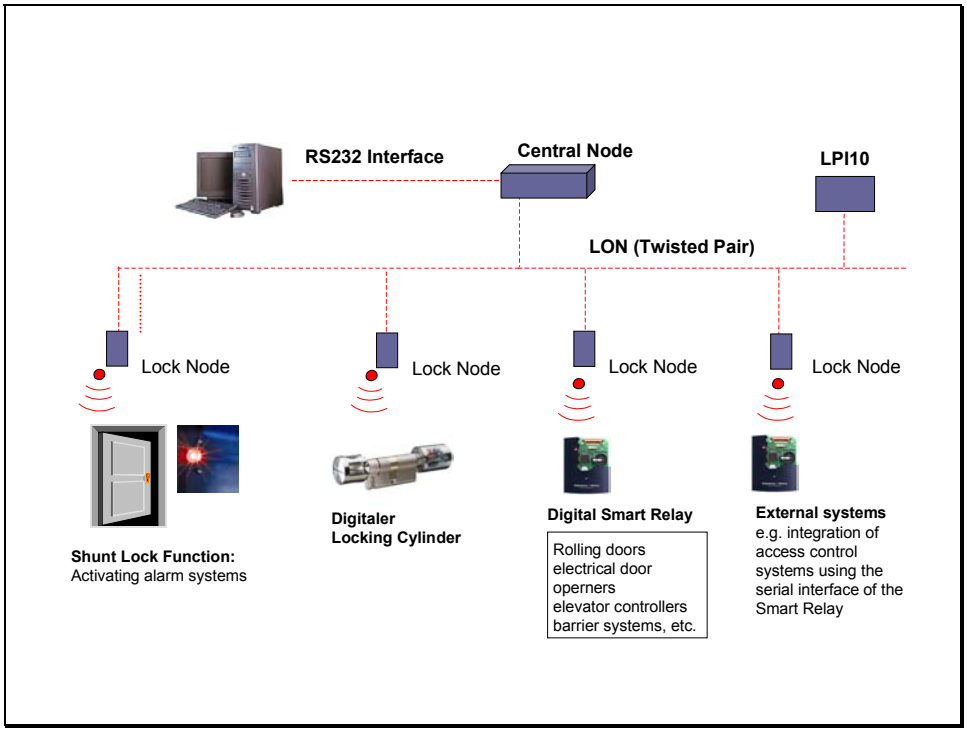
Programming the System 3060 with a laptop and SmartCD is advisable up to a certain object size or for customers with a limited number of doors, because changes in the configuration of the lockings usually do not have to made often in this case.

For medium-sized or large objects, where it happens more often that keys are lost, new transponders have to be approved, and there are organisational changes, there is the possibility of caring for and maintaining the locking system via the network. This does not necessarily mean that all doors have to be networked, however. The entire system can also be designed for mixed operation (networking/standalone).
In a networked system, it is not only possible to take care of all maintenance and programming task's from one central PC, it is also possible to obtain an overview of the current status of the entire network. For example, it is possible to check locking and door conditions, such as door open/door closed and door locked, and to display battery warnings, the access journal and burglar alarms from a central location. This makes it possible to react to an event directly from the control center.

In summary, it can be stated that using networking, it is possible to configure and monitor the entire access control system from one central PC. This means that the user can react to critical conditions in a short time.

1.1 General Information

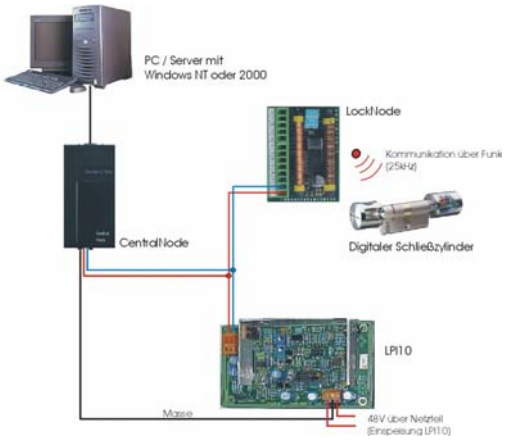
A so-called LockNode is placed next to the digital locking at a distance of about 30 cm (12 inches), depending on the particular components installed (refer to page N7). This LockNode maintains radio contact with the locking. The digital lockings do not need additionally wiring. The CentralNode forms the interface between the computer and the network.



Before starting to install the components, you should check the cable for continuity and short circuits, in order to avoid any hardware defects.

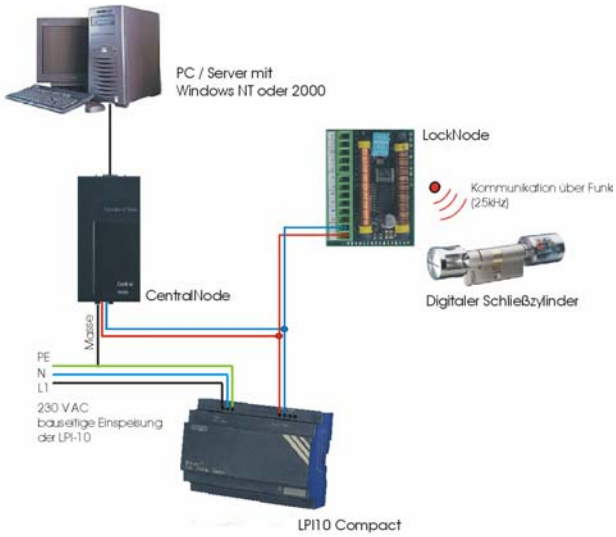
1.2 Connection to LPI-10 (Version: Open PCB With External Plug-in Power Supply)

The LockNodes are connected to the CentralNode using a two-wire line (twisted pair). The LPI-10 (version: open printed circuit board with external plug-in power supply) provides the LockNodes with voltage over the same line.



1.3 Connection to LPI-10 Compact

The LockNodes are connected to the CentralNode using a two-wire line (twisted pair). The LPI-10 (version: compact construction with 230V supply from the customer) provides the LockNodes with voltage over the same line.



2.0 The Software

If you use a PC to administer the locking system, you only need the locking plan software LDB[*1] or LSM[*2]. To access the locking system from more than one workplace, you must have LSM installed.

In network operation, the LDB[*1] software handles functions for visualisation, filtering, encoding, network management and data calibration. You can read out, change and verify all network components. Only trained personnel are permitted to install the network, in order to guarantee trouble-free function.

[*1] LDB = Lock Data Base
[*2] LSM = Locking System Management

- Please refer to the chapter on "Commissioning" in the software operating instructions for information on the system requirements for the locking plan LDB.

- Please refer to the LSM - Locking System Management handbook for information on LSM system requirements.

To operate the Network 3065, you must have a license, which depends on the size of the network. These licenses are available in the following progressive sizes:

For networks with max.	12	LockNodes
For networks with max.	48	LockNodes
For networks with max.	128	LockNodes
For networks with max.	258	LockNodes
For networks with max.	516	LockNodes
For networks with max.	1032	LockNodes

3.0 Central Node

3.1 Method of Operation

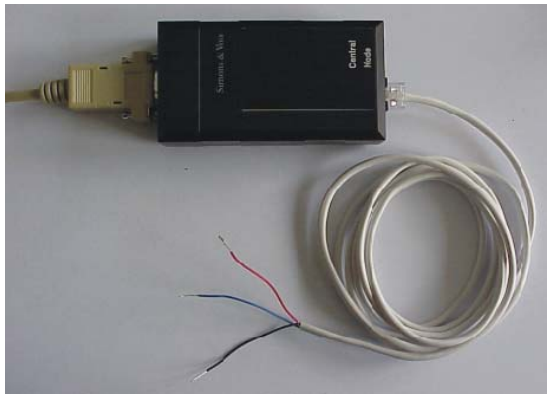
The CentralNode produces the interface between the PC and the network. One CentralNode is needed per network.

☺ To use a CentralNode in combination with LSM, please contact your trade partner or the manufacturer.

The CentralNode is connected to a free serial interface (e.g., COM1) on the PC. The ConfigDevice (or SmartCD) needed for programming transponders is connected to a different free interface on the PC (e.g., COM2). If only one interface is available, you can alternately connect the ConfigDevice (or SmartCD) and the CentralNode, depending on which you need. To do this, you must specify the device currently being used in the locking plan software. Insert the connection cable, which is delivered with the system, to the RJ-45 socket of the CentralNode.

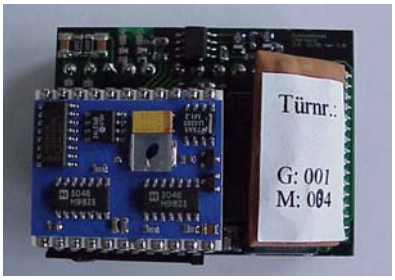
The red and blue lines on this cable are available for connection to the in-house network cable; the black line on the cable is for grounding. In order to guarantee flawless functioning of the network, the black line must be connected to the LPI-10's potential compensation. The cable's screening can be used for grounding.

☺ The CentralNode does not need a supply voltage. This is already provided by the LPI-10 over the network cable.



4.0 Lock Node

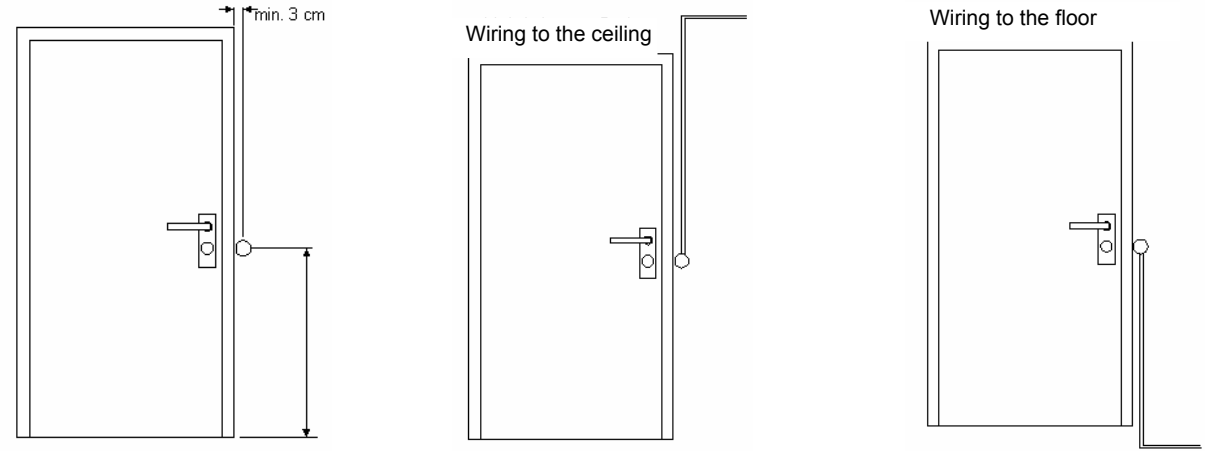
4.1 Method of Operation



The LockNode takes on all programming assignments in the network. Data is also transmitted to the digital components by radio.

4.2 Assembly Instructions

The LockNodes are pre-configured by SimonsVoss and are provided with numbers (see the picture on page N6). These numbers (GID: GroupID, M: MemberID) are entered in the set-up diagram for the building that is to be networked. During installation, assign the LockNodes in the software on the basis of this set-up diagram. Do not exchange the LockNodes, since otherwise no network connection can be made to the digital components.



The LockNodes can be built into the lighting strip next to the door in a commercially available flush-socket device or cavity socket (at least 40 mm deep) with accompanying dummy cap. You should completely remove the network cable screening in the flush socket device or cavity socket (only star-shaped wiring).
In networks with no topological structure and for BUS wiring, the screening of the respective network cables should be connected in such a way (external terminal or soldering, each with shrink sleeve) that screening is guaranteed for the entire network cable.

The terminator is then inserted at the last LockNode in the BUS wiring, and its grounding cable (green-yellow) is connected to the screening (shield) or equipotential bonding.

In order to guarantee proper radio transmission, you should maintain the following distances between the LockNode and the digital locking:

	Minimum	Maximum
LockNode to the digital locking cylinder	10 cm	30 cm
LockNode to the digital control unit	20 cm	100 cm
LockNode to the Smart Relay	50 cm	100 cm
LockNode to the activation unit	20 cm	100 cm

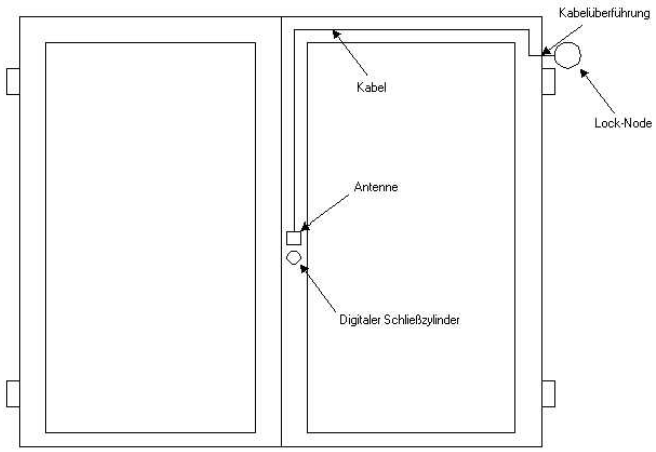
- For distances between the LockNode and the control unit of less than 20 cm or less than 50 cm between the LockNode and the Smart Relay, we ask that you contact your dealer or the manufacturer.

- The LockNodes must be built according to the layout plan drawn up during planning. The plan indicates the position of the LockNodes and specifies the group and member IDs. This information is printed on the LockNode. All necessary wires must be connected to the LockNode terminal strip. (Network cable connection: terminals 1 and 2. The polarity is not relevant).

4.3 Antenna Extender

Since the standard range of the LockNode is not sufficient for double doors, a LockNode with an extended antenna must be used in this case. The extended antenna is mounted in the door (in the immediate vicinity of the cylinder) and connected to the LockNode via a cable transfer on the door.

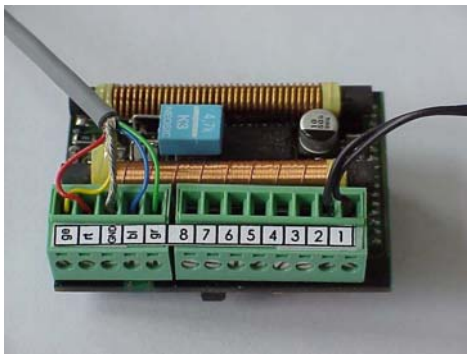
- To guarantee that the radio transmission functions correctly, we recommend that you provide a plastic inspection flap at the level of the antenna.



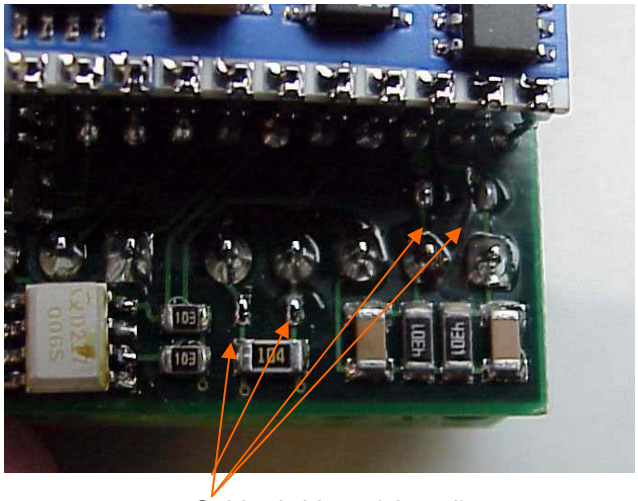
- You can always attain wider ranges by using FH versions.

- Make sure that the cable of the extended antenna is exactly the length needed. You should always cut off any extra cable length.

Connect the network cable to terminals 1 and 2 of the LockNode. If you need an antenna extender because of a double door, connect the antenna extender cable to the terminals, according to the line colours.



When connecting the extended antenna, also remove the four solder bridges (0Ω resistors) on the LockNode printed circuit board. Otherwise, the LockNode cannot function with the extended antenna.



Solder bridges (closed)

To open the solder bridges, please use an appropriate tool (adjustable soldering iron and unsoldering suction pump).

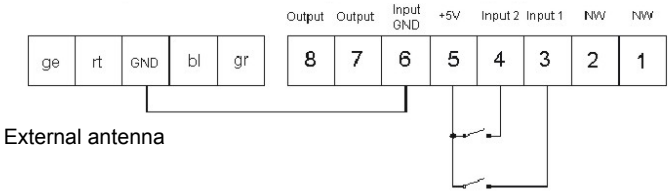
Only authorised personnel should install and open the solder bridges.

4.4 LockNode Inputs and Outputs

Terminals 3 to 8 are available for floating inputs or one output. The inputs transmit the state of the door or lock contact, for example. However, you can also incorporate external systems, such as motion detectors, photoelectric barriers, etc., into the system and then also report their signals to the central computer. You can use the output to pass on signals to external systems, such as heating, light, etc.

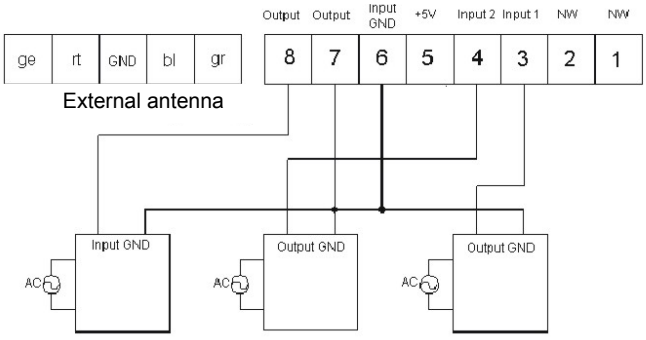
You can use the internal power supply of the node to connect switches or contacts without a separate power supply and without a ground connection.

Connection of contacts which don't have their



Follow the technical specifications for the inputs or the output when connecting them. Refer to the data sheet for this information.

Connection of contacts with own power supply



5.0 LPI-10

5.1 General Warnings

The LPI-10 is a regulated power supply, designed for use in single-phase AC power networks. Furthermore, it is a built-in device, so that it is intended for installation in a distribution box or control cabinet. You must comply with the relevant DIN/VDE regulations or the regulations that apply to your country when installing the device.
You must connect the supply voltage in compliance with VDE 0100 and VDE 0160. You must provide a protective device (fuse) and a power supply disconnecting device.
Correct and safe operation of this device requires proper transport and professional storage, assembly and installation.

5.1.1 Risk of Electric Shock

Operation of electrical devices inevitably requires that certain parts of these devices carry hazardous voltage. Improper handling of these devices can therefore result in death or serious bodily injury, as well as in considerable property damage.

5.2 LPI-10 (Version: open printed circuit board with external plug-in power supply)

5.2.1 Method of Operation

You need at least one LPI-10 for each network segment in order to supply the LockNodes. The LIP-10 also needs a separate supply voltage of 48 Volts DC.

There are two models available for this, depending on the size of the network:

- LPI-10 with 48V plug-in power supply for max. 40 LockNodes
- LPI-10 with 48V plug-in power supply for max. 62 LockNodes

Larger networks use proportionately more LPI-10 modules.

5.2.2 Assembly Instructions

The LPI-10 is intended for installation in distribution boxes with DIN rails. You will also need an outlet for the plug-in power supply of the LPI-10. Depending on the structural situation and number of groups, you can also put several power supplies and routers in one distribution box.

Connect the network cable (twisted pair) here. You can also lay a network cable to the router (if there is one). Connect the cable to terminals 17 and 18 there. An additional network cable goes from the router to the LockNodes.

Connect the plug-in power supply to these terminals. Make sure that the polarity (+/-) is correct. This is printed on the connecting terminals. Ground the LPI-10 on the middle terminal.

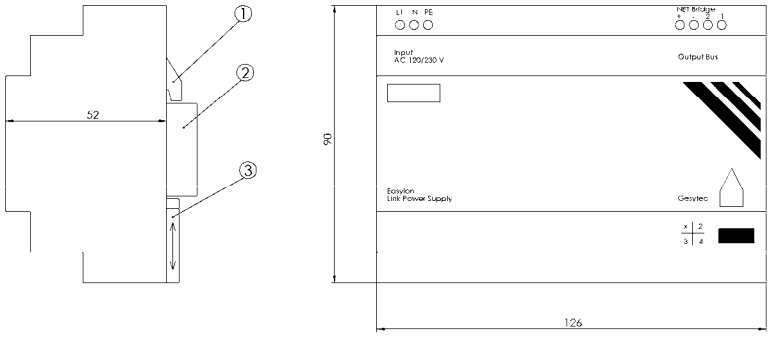
- Build the LPI-10 into the separate segments in such a way that there is voltage of at least 35V DC on each LockNode.
- Consequently, the installation location depends on the number and particular distribution of the LockNodes in the corresponding segment.
- If it is not possible to guarantee voltage of 35 VDC at each LockNode with one LPI-10, you must install a repeater (including power supply) and an additional LPI-10 (including power supply) in the segment.
- The LPI-10, as it comes from the factory, does not have any over voltage protection. For this reason, this protection should be already provided for by the customer.
- When commissioning the LPI-10 and the network, you must make sure that the line voltage that is applied is 230V~ (+/- 10%). Higher or lower line voltage input to the LPI-10 can lead to disturbances in the network.

5.3 LPI-10 Compact (Version: compact construction with 230V power supply from the customer)

5.3.1 Installation

Only a qualified expert who is familiar with and who complies with the generally applicable rules of the technology and the regulations and standards valid at the time is permitted to assemble and wire the LPI-10.

The device can be snapped on to DIN EN 50022-35 x 15 and DIN 50022-35 x 7.5 standard mounting rails. To snap the device in, hang it in with the catch ① in the top-hat rail③ and press until the spring ② snaps into place (see following drawing). If it is too hard to snap it in, loosen the spring ② somewhat. To remove it from the DIN rail, use a screwdriver to loosen the spring ② in the direction of the arrow and remove the device.



To ensure proper heat dissipation, you must install the device vertically, so that the input and output terminals are at the top. There should be at least 5 cm (2 inches) of clearance above and below the device in order to prevent interference with the air circulation.

- Before beginning installation or maintenance work, switch off the system's main switch and ensure that the system cannot be switched on again. During maintenance work, provide a suitable disconnection device to disconnect the unit from the electrical supply circuit.
  Use a screwdriver with a blade 3 mm (approximately 0.12 inches) wide. You do not need any wire end ferrules for the terminals. You can use lines up to thickness of 1 x 2.5 mm ^{2} or 2 x 1.5 mm^2.

5.3.2 Method of Operation

You need at least one LPI-10 for each network segment in order to supply the Lock-Nodes.
The LPI-10 (new construction) has 3 terminals for connection to the supply voltage:

Terminals:
INPUT AC 230V:
L1: 230V~ connection
N: 230V~ connection
PE: Potential compensation connection

OUTPUT BUS:
NET+: Network cable connection
NET-: Network cable connection

BRIDGE 1 + 2:
- For a network with no topological structure or with a star-shaped structure, bridge the "Bridge 1-2" connection
- You are not permitted to bridge this connection if you are using a bus topology.

5.3.3 Assembly Instructions

The LPI-10 is intended for installation in distribution boxes with DIN rails. Clamp the voltage supplied from outside to the terminals marked for that purpose. Depending on the structural situation and number of groups, you can also put several power supplies and routers in one distribution box.

Connect the outside 230V~ plug-in power supply to these terminals. This is printed on the connecting terminals. Ground the LPI-10 on the terminal labeled PE.

Connect the network cable (twisted pair) here. For BUS wiring, the connection between "Bridge 1-2" stays open, but for other wiring you must insert a bridge here.
You can also lay a network cable to the router (if there is one). Connect the cable to connecting terminals 17 and 18 there. An additional network cable goes from the router to the LockNodes.

Build the LPI-10 into the separate segments in such a way that there is voltage of at least 35V DC at each LockNode.
Consequently, the installation location depends on the number and particular distribution of the LockNodes in the corresponding segment.

If it is not possible to guarantee voltage of 35 VDC at each LockNode with one LPI-10, you must install a repeater (including power supply) and an additional LPI-10 (including power supply) in the segment.

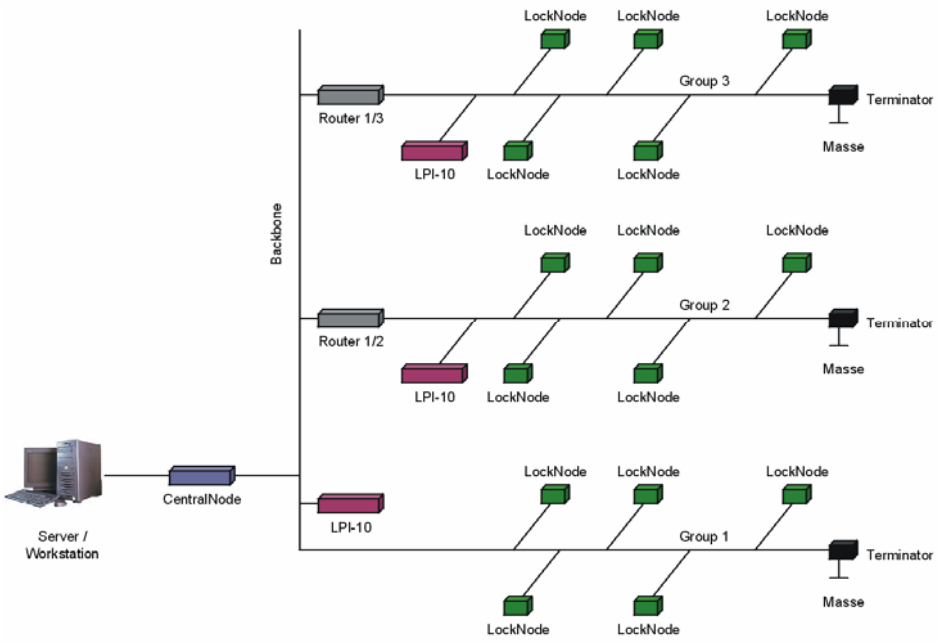
The LPI-10, as it comes from the factory, does not have any over voltage protection. For this reason, this protection should be already provided for by the customer.

6.0 Router

6.1 Method of Operation

Routers are needed in order to separate individual segments, such as floors or buildings, from one another in large networks. From the entire data stream that arrives at one side, they are able to filter out the data that is intended for the segment lying behind them (data segmentation). Because the routers receive a Group ID, they must be configured by SimonsVoss.

Example:



One segment can have a maximum of 62 LockNodes. As soon as this number is exceeded, you must open a new segment with a router and an additional LPI-10 module + plug-in power supply. A network can have a maximum of 63 segments. In large networks, you should choose the segments to fit the structural conditions, for example, one segment per building or floor.

- Routers need a 230 V AC power supply from the customer (outlet).

- Routers, as they come from the factory, do not have any over voltage protection. For this reason, this protection should be already provided for by the
customer.

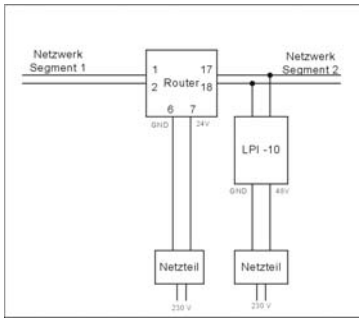
- If elevators are to be integrated into the networking, they are not permitted to be installed in the backbone. Instead, they must be separated from the backbone by a router.

6.2 Assembly Instructions

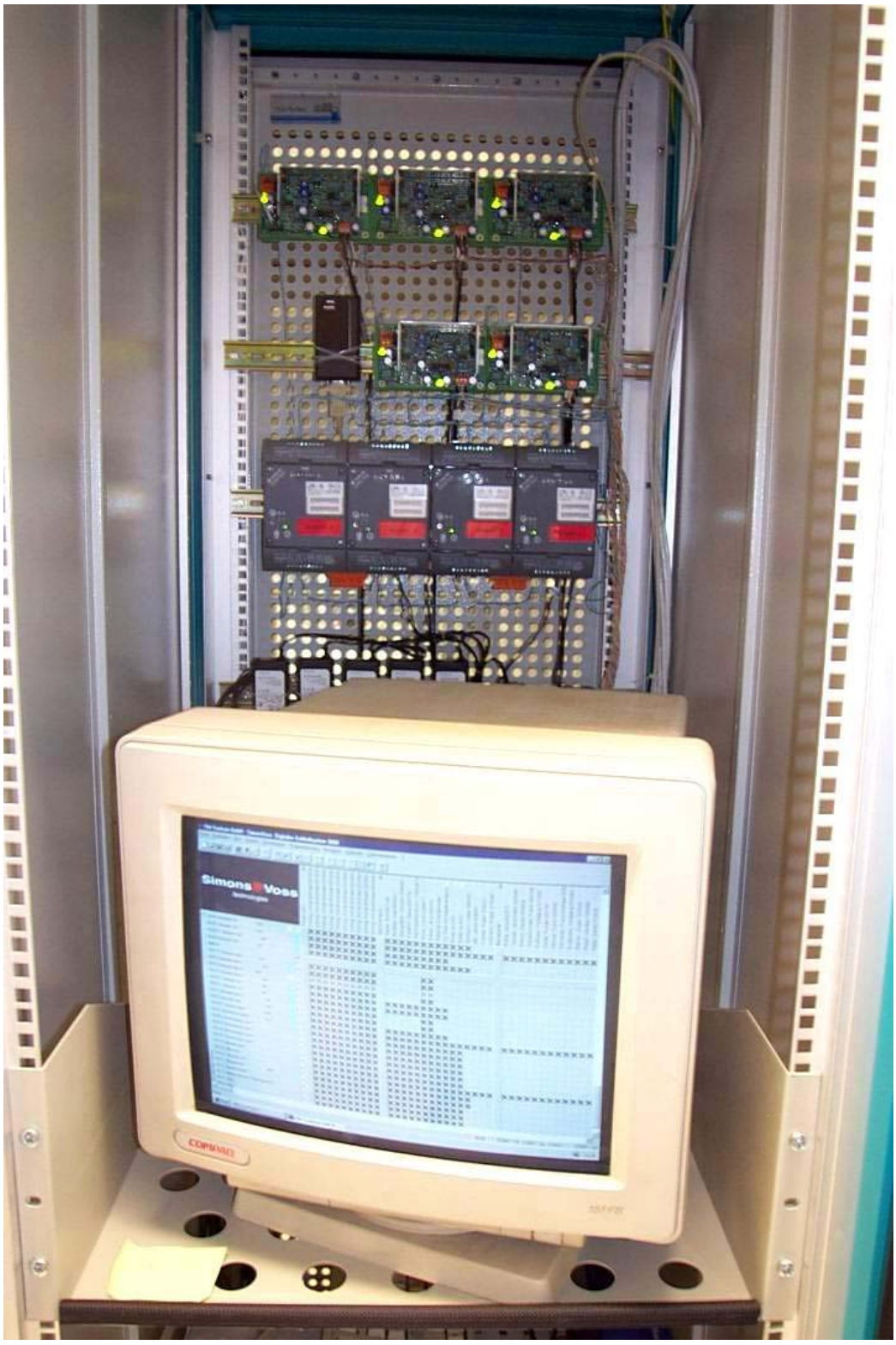
You can attach routers to a DIN rail. Please refer to the following figure for the connection assignments:

1+2	Input A of network
3+4	Additional input A (internal bridges from 1-3 and from 2-4)
5	Not used
6+7	Supply voltage: power supply connection
8+9	Additional supply voltage (internal bridges from 6-8 and from 7-9)
10-14	Not used
15+16	Output B of network
17+18	Additional output B (internal bridges from 15-17 and from 16-18) This output can be used for connecting the LPI-10, for example.

- Connect the inputs of all routers in parallel. It is very important that you do not confuse input A and output B with one another.



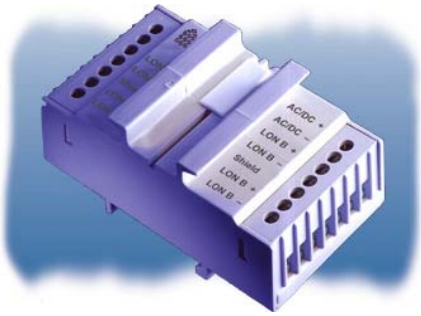
6.3 Installation Example



7.0 Repeater

7.1 Method of Operation

The repeater increases the allowable communication distance by regenerating the signals. Unlike routers, the repeater does not have a group ID, so it does not have to be configured by SimonsVoss.



7.2 Assembly Instructions

Install it in a small housing that is suitable for DIN rail assembly. Connect the (LON) network lines to terminal screws on both sides. The power supply – which can be either AC or DC – is on one side of the housing. Feed the cable screen through to the opposite side.

The repeater always needs a separate power supply, which is not included in the delivery!!!

Repeaters, as they come from the factory, do not have any over voltage protection. For this reason, this protection should be already provided for by the customer.

8.0 Terminators

To avoid disturbances, you must use a so-called terminator (pull-up resistor) in the bus system as the segment termination. Connect this pull-up resistor to terminals 1 and 2 of the last LockNode and also to the network equipotential bonding.

9.0 Network Cable

9.1 General Information

Every LockNode is networked with one line consisting of two twisted wires (twisted pair). The data and the supply voltage are both transmitted over this line (see Fig. on page N2 or N3). An LPI-10 or LPI-10 Compact module feeds the twisted pair line with voltage (approximately 48 V DC).

9.2 Cable Laying

There are almost no restrictions placed on the cable laying when the given cable types are used. As a matter of principle, however, placement parallel to cables with strongly pulsating high voltage should be avoided. If, however, due to structural reasons, it is possible to use only cable that has already been laid but which either does not meet the required demands or which meets them only partially, the result can be interference due to radiation from other cables or systems. This interference can affect the performance capability of the network or can even lead to a complete network blackout. Therefore, it is important in these cases to pay special attention to cables or external systems that are in the vicinity of the transmission cable. This means high power machine systems, elevators, microwave systems, or transmission systems, for example.

- Connect the shields of all network cables to one another. Normally, these are connected to the potential compensation on the LPI-10.

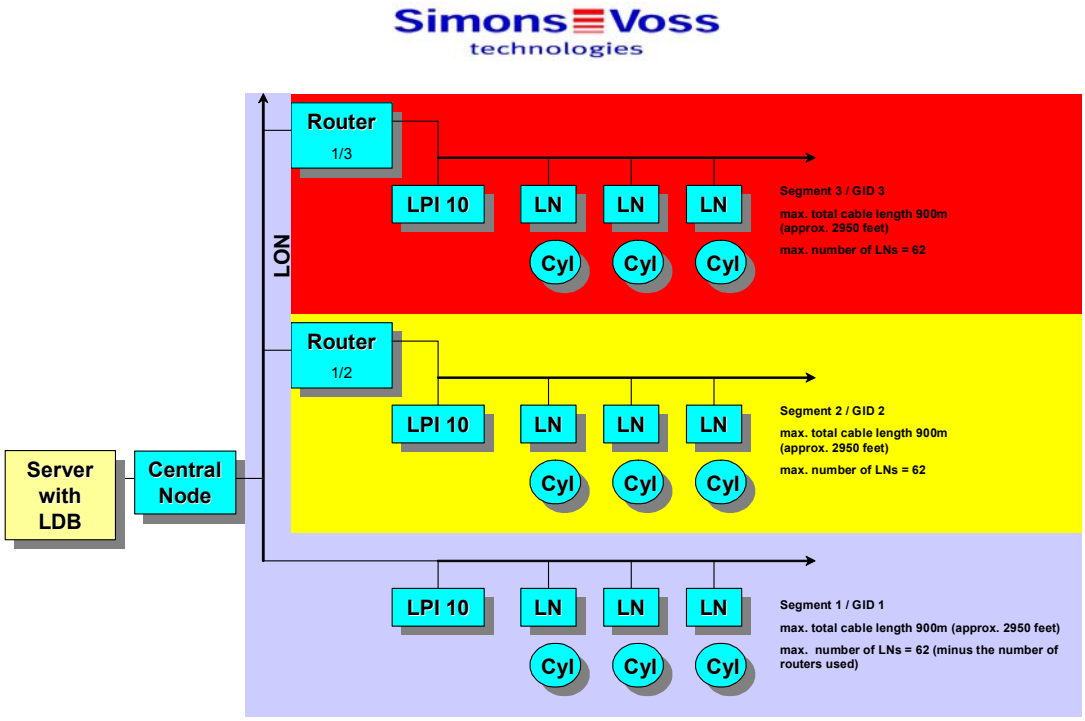
9.3 Cable Types

The type cable that you use depends on the following factors:

1. Total cable length (from the CentralNode to the last LockNode)
2. Cable length between the LockNodes
3. Network topology: wiring plan (star or bus system)

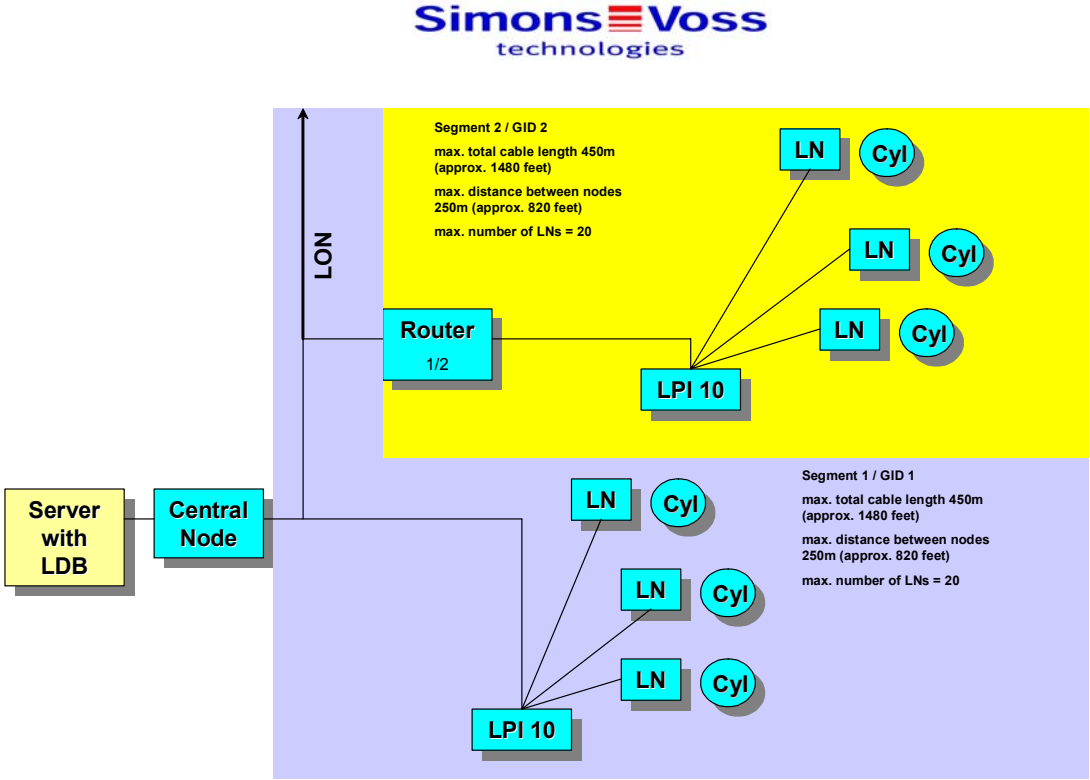
	With no topology	**With no topology**	**Bus topology with terminators**
	Total length	*Distance between nodes*	*Total length*
JY (ST) Y 2x2x0.8	500 m	320 m	900 m
Category 5	450 m	250 m	900 m

9.4 Bus-Shaped Cabling (Example)



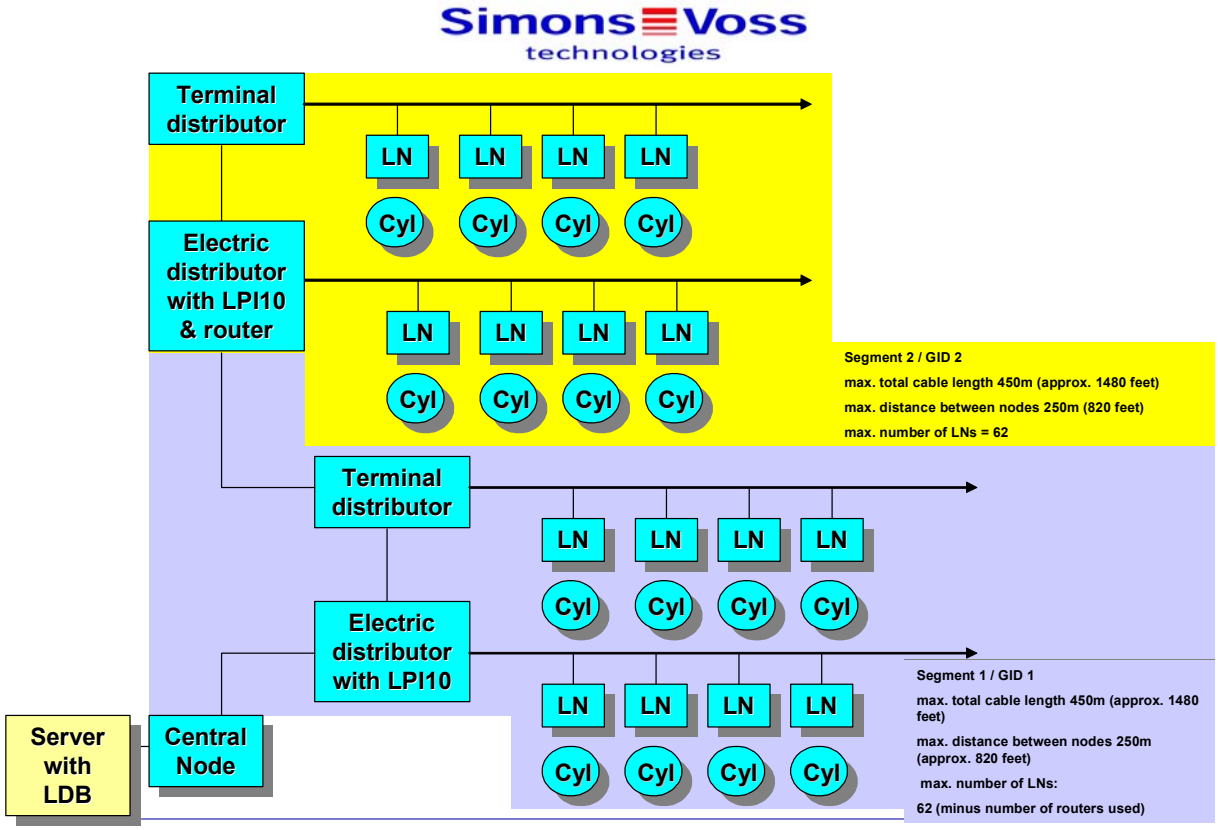
Bus System Cabling (Values for Cat5 Cable) 2

9.5 Star-Shaped Cabling (Example)



Star-Shaped Cabling (Values for Cat5 Cable) 1

9.6 Cabling With no Topology (Example)

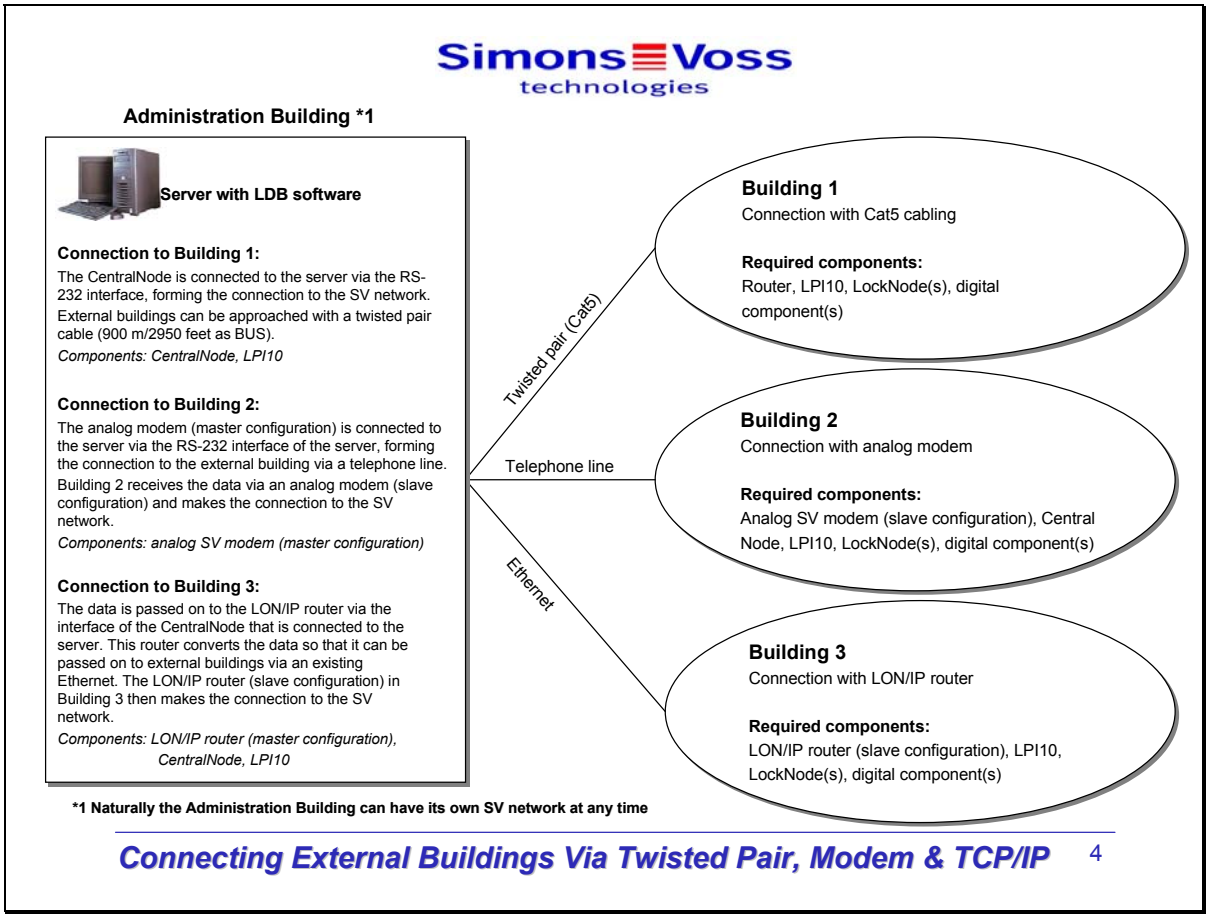

Simons Voss technologies
Terminal distributor
Electric distributor with LPI10 & router
Terminal distributor
Electric distributor with LPI10
Server with LDB
Central Node
LN
Cyl
Segment 2 / GID 2
max. total cable length 450m (approx. 1480 feet)
max. distance between nodes 250m (820 feet)
max. number of LNs = 62
Segment 1 / GID 1
max. total cable length 450m (approx. 1480 feet)
max. distance between nodes 250m (approx. 820 feet)
max. number of LNs:
62 (minus number of routers used)

Cabling With no Topology (Values for Cat5 Cable)

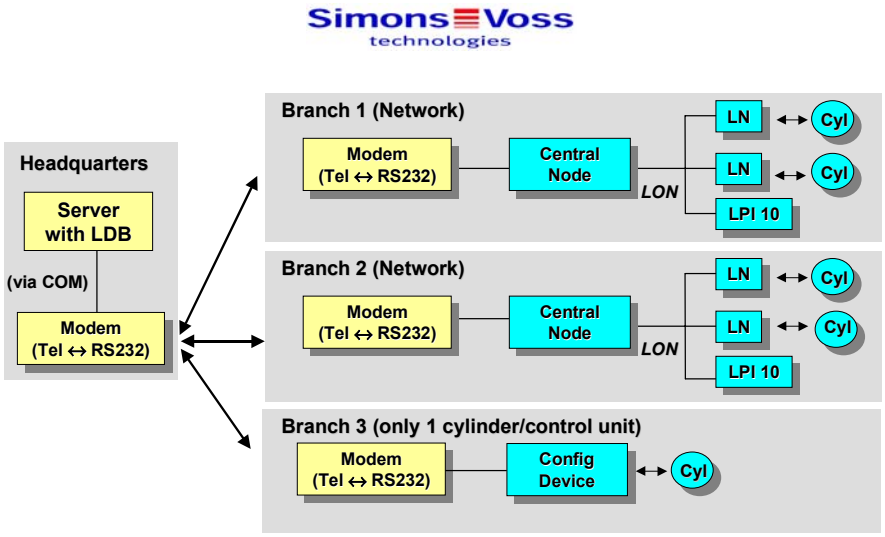
10.0 Planning Examples

10.1 Connecting External Buildings via Twisted Pair, Modem & TCP/IP

Remark: The planning and implementation of the following planning examples must be carried out by SimonsVoss. This chapter therefore offers only a short description of networking via modem and TCP/IP router.


SimonsVoss technologies
Administration Building *1
Server with LDB software
Connection to Building 1:
The CentralNode is connected to the server via the RS-232 interface, forming the connection to the SV network. External buildings can be approached with a twisted pair cable (900 m/2950 feet as BUS).
Components: CentralNode, LPI10
Connection to Building 2:
The analog modem (master configuration) is connected to the server via the RS-232 interface of the server, forming the connection to the external building via a telephone line. Building 2 receives the data via an analog modem (slave configuration) and makes the connection to the SV network.
Components: analog SV modem (master configuration)
Connection to Building 3:
The data is passed on to the LON/IP router via the interface of the CentralNode that is connected to the server. This router converts the data so that it can be passed on to external buildings via an existing Ethernet. The LON/IP router (slave configuration) in Building 3 then makes the connection to the SV network.
Components: LON/IP router (master configuration), CentralNode, LPI10
Twisted pair (Cat5)
Telephone line
Ethernet
Building 1
Connection with Cat5 cabling
Required components:
Router, LPI10, LockNode(s), digital component(s)
Building 2
Connection with analog modem
Required components:
Analog SV modem (slave configuration), Central Node, LPI10, LockNode(s), digital component(s)
Building 3
Connection with LON/IP router
Required components:
LON/IP router (slave configuration), LPI10, LockNode(s), digital component(s)
*1 Naturally the Administration Building can have its own SV network at any time
Connecting External Buildings Via Twisted Pair, Modem & TCP/IP
4

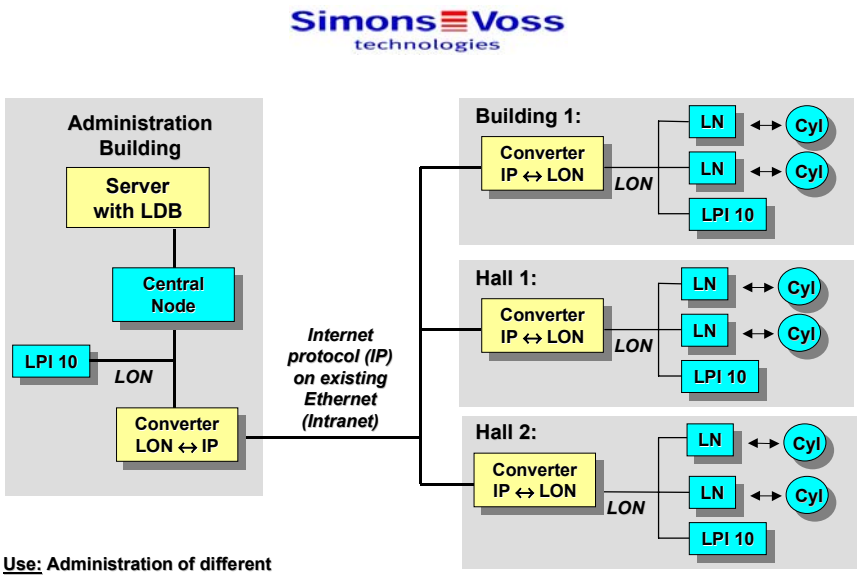
10.2 Network via Modem



Use: Administration of many branch offices in different locations via one server/PC (via normal telephone network)

Network via Modem 5

10.3 Network via Ethernet



Use: Administration of different buildings/halls (in one location) via existing Ethernet (Intranet)

Network via Ethernet (IP-LON router) 7

11.0 Security

Because the Network 3065 records and logs critical data, it must be reliably protected from unauthorised accesses. This demands a great deal from the system as far as information and manipulation security.

11.1 Secure Communication Between the Network Nodes

Network communication is protected against data tapping in the following ways:

- In order to prevent the data stream from being monitored, the data is encoded for transmission.
- The encoding also provides sufficient protection during professional attacks using cryptoanalysis.

11.2 Automatic Tests of Separate System Components

Because separate components can be distributed widely across parts of a building, a malfunction, manipulation and forcing of a door must be detected and reported to the central PC automatically.

Important: If a door is equipped with a forced opening alarm function, it must have a lockcontact.

All nodes report to the central PC at time intervals that can be configured. These time frames can also be selected to be variable for certain time frames, so that, for example, critical doors report more often at night than during the day.

11.3 Alarms

Alarms are messages that require a prompt response (such as in case of a burglar or fire). If the same alarm occurs repeatedly, it is only reported once, in order to keep a better overview and to reduce the load on the alarm control centers.

12.0 Answers to the Most Common Questions Regarding the Network

- *Is it possible to use a cable that is already there for a twisted pair?*

Yes, you can use a cable that is already there, as long as it holds two strands that are not in use yet. However, the maximum range that can be attained with this cable is considerably less than that reached with special Twisted-Pair cables, depending on the nature of the cable.

- *How long can a line be with a twisted pair?*

Under optimum conditions, the maximum distance that can be attained is approximately 900 m (roughly 2953 feet). By using routers and repeaters, however, this distance can be extended to practically any length.

- *Are there restrictions on the line topology?*

In principle, the network is designed for mixed topology, which means that star and series interfacing can be mixed in any combination and adapted to the local conditions. In practice, there are restrictions regarding range and reaction time, depending on the set-up used and the line lengths. Therefore, if structured cabling is possible, especially in new buildings, it is better to pick a topology, usually BUS cabling.

- *After what line length should I use a router or repeater?*

The number and position of routers/repeaters used depends greatly on the structure of the planned network. If different buildings are networked together, however, a router should always be provided.

- *What is a router?*

A router is needed in order to separate individual segments (such as floors or buildings) from one another in large networks. From the entire data stream that arrives at one side, it can filter out the data that is intended for the segment lying behind it (data segmentation). Routers must be configured by SimonsVoss before they are installed. Routers require a 230 V~ connection (outlet) via a separate plug-in power supply for their own supply voltage.

- *What is an LPI-10?*

The LPI-10 is the power supply for the Twisted-Pair LockNodes. It consists of an interface module and the power supply. The interface module prevents attenuation of the data packets by the power supply and a defect of the supply voltage when there is a short circuit on the network. The required input voltage of 48 V direct current is supplied either by a plug-in power supply that can feed a maximum of 40 LockNodes, or a larger plug-in power supply that is designed for a maximum of 62 LockNodes.

- *What is an LPI-10 Compact?*

An LPI-10 Compact essentially corresponds to the LPI-10, but with the difference that the LPI-10 Compact is always designed for 62 LockNodes and does not need a separate plug-in power supply. It is connected directly to the 230V~ at the customer.

- *How many LPI-10 or LPI-10 Compact modules are needed?*

At least one LPI-10 or LPI-10 Compact must be used for each segment (divided by routers). The number depends on the particular segment structure. In principle, however, it can be said that each LockNode in the segment must be supplied with at least 35 V DC in order to guarantee perfect operation.

- *Where should the LPI-10 or LPI-10 Compact be placed in the segment?*

At least one LPI-10 or LPI-10 Compact must be used for each segment (divided by routers). The position of the LPI-10 or LPI-10 Compact depends on the particular segment structure. In principle, however, it can be said that placement in the middle of the segment is the most sensible.

If you have other questions, please contact your trade partner or the manufacturer.

13.0 Data sheet

CentralNode	Dimensions	100 x 54 x 30 mm [L/W/H]	
	Network connecting cable	200 cm (approx. 6.6 feet)	
	RS232 connecting cable	300 cm (approx. 9.9 feet)	
LockNode	Dimensions	53 x 40 x 20 mm [L/W/H]	
	Input	Input voltage range	5–24 V
	Output:	Maximum switching voltage	24 V
		Maximum switching current	300mA
		Intrinsic resistance (AN)	1.5Ω
Router	Dimensions	120 x 100 x 40 mm [L/W/H]	
	Input voltage	24 V DC	
Router plug-in power supply	Dimensions	90 x 56 x 81 mm [L/W/H]	
	Output voltage	24 V DC	
LPI-10 (Version: open printed circuit board with external plug-in power supply)			
	Dimensions	135 x 80 x 60 mm [L/W/H]	
	Input voltage	48 V DC	
	Output voltage	approx. 41-42 V DC	
Plug-in power supply 40	Dimensions	60 mm x 80 mm [W/H]	
	Input voltage	230 V AC	
	Output voltage	48 V DC	
Plug-in power supply 64	Dimensions	107 x 45 x 25 mm [L/W/H]	
	Input voltage	230 V AC	
	Output voltage	48 V DC	

LPI-10 (Version: Compact)

Input quantities

Nominal input voltage U_E	AC 120 / 230V
Input voltage range	AC 85 to 264V
Nominal frequency range	50/60Hz, 47 to 63Hz
Power failure buffering	> 50 ms at U_E=195V
Nominal input current I_E	0.8 / 0.5A
Making current impulse	≤30mA
Efficiency η	≥ 75% in operation at nominal value at 230 V AC
Recommended circuit breaker (IEC898) in the power supply lead	from 6A Char. D from 10A Char. C from 16A Char. B

Output quantities

Nominal output voltage U_A	DC 41.5 V ±2%
Residual ripple	< 100mV_{ss} at 10kHz < f < 200KHz
Spikes (switching peaks)	< 200mV_{ss} at 200KHz < f < 1MHz
Nominal output current I_A	1A at U_E 85 to 195V 1.3A (1.5A max. permitted continuous current from U_E 195V
Overload protection typically at	1.6A; continuous short-circuit-proof with pulsating restart attempt
Overvoltage protection typically at	54 V
Start and restart time	5s < t < 10s

Environmental Conditions

During transport/storage	-40° C to +70° C (-40° F to +158° F)
During operation	0° C to +40° C (32° F to +104° F)
Rel. air humidity	5 to 95%, w/o moisture condensation

Security

Degree of protection to EN 60529	IP20

Protection class to VDE 0106 Part 1	I (with ground terminal)
Electrical isolation, primary/secondary	SELV to EN 60950
Electromagnetic compatibility	
Emitted interference (EN 500081-1)	Class B to EN 60950
Noise immunity (EN 50082-2)	EN 61000-4-2/3/4/5/6, level 3
Weight	
Weight	Approx. 0.5 kg
Approvals	
Approvals	CE (98/336 EEC, 73/23 EEC)

Programming Transponder 3067

State of: June 2006

SimonsVoss technologies

Programming Transponder 3067

Content

1.0 Introduction 3

2.0 Backup Card 3

3.0 Programming Notes 4

- 3.1 Error Messages 4
- 3.2 Initial Programming 4
- 3.3 Reading Out a Transponder 5
- 3.4 Adding a New Transponder 5
- 3.5 Emergency Opening 6
- 3.6 Blocking a Lost Transponder 6

4.0 Loss of the Programming Transponder 7

5.0 Data Sheet 7

1.0 Introduction

The Programming Transponder 3067 is used for programming Digital Locking Cylinder 3061 and Transponder 3064 devices. You can use it to perform the following actions:

- Program the system for the first time
- Make changes to the authorisations
- Block lost transponders
- Determine the ID number of a transponder

It is not possible to read out the locking cylinder with the Programming Transponder. Each transponder receives its own ID number and secret password when the system is programmed for the first time. This allows the locking cylinders to distinguish between the different transponders.

The Programming Transponder takes care of this job. It assigns a consecutive ID number to the transponders, beginning with 1. The next transponder receives the number 2, and so on. You can program a maximum of 99 transponders and a maximum of 250 lockings with a program transponder.
While the Programming Transponder is carrying out the programming, the locking cylinders are also learning the secret password, as well as which transponders will be authorised in the future.

2.0 Backup Card

The entire system is protected by a secret password that is saved at the factory on the Programmer Transponder 3067. The system password is stored on the backup card. The password is covered by a scratch panel and does not have to be scratched free for programming. Keep this backup card in a safe place and make sure it is not accessible to third parties. If the backup card is lost, it may be necessary to replace the entire locking system.

3.0 Programming Notes

Always position only one locking cylinder in the immediate vicinity of the Programming Transponder during programming. All other components must be at a distance of at least 1 m (3.3 feet).

3.1 Error Messages

If you receive one of the following signals when not expected during the programming, there has been an error.

- Light emitting diode (LED) blinks red 1x:
  Action: Correct the distance to the cylinder or transponder and try again.

- LED flickers and then blinks red 2x.
  You have tried to authorise a transponder in more than 3 different locking systems. (A transponder can be authorised for a maximum of 3 different locking systems).

- LED flickers and then blinks red 3x:
  You have tried to program more than the maximum allowable number of transponders or cylinders.

- LED flickers and then blinks red 4x.
  You have tried to authorise a transponder for a cylinder that does not belong to your locking system.
  or
  The programming transponder button was pressed too long.

3.2 Initial Programming

The following programming steps must be done very quickly, because otherwise the Programming Transponder automatically shuts down, which interrupts the programming.

Be absolutely sure to maintain a minimum distance of 1 meter (3.3 feet) from the locking cylinder to the Programming Transponder when carrying out steps 1 and 2.

1. Briefly press the Programming Transponder button once. The light emitting diode then blinks green.

2. Operate the transponder that you want to program at a distance of from approximately 10 to 20 cm (4 to 8 in.) to the Programming Transponder and wait until the light emitting diode on the Programming Transponder lights green for three seconds. If you want to authorise another transponder, repeat step 2.

3. Once you have authorised all transponders, hold the Programming Transponder near the inner knob of the cylinder (long knob) and briefly press

its
button one time. Attention: you must press the button during the LED's blinking phase. The data is then transferred. The locking cylinder makes several signal tones during this part of the programming. If the programming was successful, the cylinder couples and the LED on the Programming Transponder lights green.

4. Perform a test to see whether all of the transponders that you have programmed function perfectly.

5. Follow the same procedure to program additional locking cylinders.

3.3 Reading Out a Transponder

In order to be able to block a lost transponder for a specific locking cylinder, you need its ID number. We recommend that you create a list containing the name of the owner and the accompanying ID number of the transponder. You can determine this with the Programming Transponder:

1. Briefly operate the Programming Transponder until it blinks green.

2. Hold the transponder whose ID number you want to read out near the Programming Transponder. Briefly operate the transponder. The LED on the Programming Transponder lights green for approximately 3 seconds.

3. Press the transponder button again. The LED lights yellowish for approximately 2 seconds.

4. The ID number of the transponder is shown by the different coloured blinking of the LED.
   Red blinking indicates the tens and green blinking indicates the ones.

   Example: If the ID number of the transponder is 25, the LED blinks red 2x and then green 5x. If the ID number has only one digit, only the green LED blinks.

5. Once the ID number has been determined, the LED on the Programming Transponder lights yellowish again.

3.4 Adding a New Transponder

If you want to authorise a new transponder, proceed in the same way as for the initial programming. You do not have to repeat the procedure for reading in transponders that were already authorised for locking.

3.5 Emergency Opening

It is possible to perform an emergency opening with the Programming Transponder. Proceed as follows:

1. Press the Programming Transponder button briefly one time. Then the LED blinks green.

2. Hold the Programming Transponder at a distance of approximately 10 to 20 cm (approximately 4 to 8 inches) from the locking cylinder and briefly press the button.
   Attention: you must press the button during the LED's blinking phase.

3.6 Blocking a Lost Transponder

The procedure depends on whether or not you know the ID number of the lost transponder. If you do not know it, proceed as follows:

1. Press the Programming Transponder button until the light emitting diode blinks red.

2. Hold the Programming Transponder near the inner knob of the cylinder (long knob) until the LED lights green for approximately 3 seconds and the cylinder couples.

3. You have now deleted all authorised transponders and must reprogram then as described in Chapter 3.2.

If you know the ID number, you can block this specific transponder with the following steps:

Note: It is important that the steps be executed quickly for this procedure, too. Memorise the ID number of the transponder so that you can enter it immediately in the
following steps. Like when reading out the number, the input is done in tens (red) and ones (green).

1. Press the Programming Transponder button until the light emitting diode blinks red. Then release the button.

2. Then repeat the procedure and wait until the LED lights red. Immediately (red LED must still be lit) press the Programming Transponder button the appropriate number of times to enter the number of tens (only if there are more than nine transponders).

3. The LED now begins to light green. Now enter the number of ones in the same way (now the green LED must still be lit).

4. The Programming Transponder repeats the ID number that you enter as a check. First the LED briefly lights yellowish. Then the Programming Transponder outputs the ID number with red and green blinking. The color then changes back to yellow and finally the LED blinks green.

5. If the displayed number is correct, hold the Programming Transponder near the inner knob of the cylinder (long knob) and press its button.

6. Then the data transfer takes place (signal tones on the cylinder). Wait until the LED has lit green for 3 seconds and the cylinder has coupled. The data transfer is not completed until this happens.

4.0 Loss of the Programming Transponder

Get your backup card and contact your dealer. You will receive a new Programming Transponder, which you first must reauthorize for your cylinders.

To do this, proceed as follows:

1. Hold your new Programming Transponder in front of a cylinder and press its button twice. The LED lights green for approximately 3 seconds and the cylinder couples.

2. Then hold your new Programming Transponder in front of the same cylinder, but this time press its button only once.

3. The light emitting diode blinks yellowish and goes out. The cylinder couples and the LED lights green for approximately 3 seconds.

4. Repeat steps 2 and 3 for all other cylinders in your locking system.

5. Once you have authorised the new Programming Transponder on all cylinders, press its button until the LED stops blinking.

6. The new Programming Transponder is now ready to use.

5.0 Data Sheet

Housing	Material	Plastic
	Colour	Grey
	Dimensions	58 x 38 x 12.3 mm

PalmCD2 Programming Device

State of : September 2004

Simons Voss technologies

PalmCD2 Programming Device

Content

1.0 Introduction _____ 3
2.0 Commissioning _____ 3
3.0 Programming with the PC or Laptop _____ 3
4.0 Programming with the Palm Organizer _____ 4
5.0 Setting Up the PalmCD2 With Transponder Function _____ 4
6.0 Data Sheet _____ 4

1.0 Introduction

The PalmCD2 is a programming device that was developed especially for operation on a PC/Laptop or in combination with a Palm m5xx or Palm Tungsten W, or T3 Organiser. It makes it very easy to program and read out all digital components of the 3060 system. You can also use the Palm to match up your personal data (addresses, calendar, etc.)

2.0 Commissioning

Insert the two batteries into the battery compartment. Make sure that the polarity is correct. Do not use storage batteries.

ATTENTION:
The battery fitted in the cylinder can, in the case of inappropriate treatment, represent a fire or bums hazard! Do not recharge, open, heat to more than 100°C or incinerate! Replace battery only with type AAA 1.5 V. Use of a different type battery can present a fire and explosion risk!

Install the PalmLDB on the Palm m5xx or Palm Tungsten W, or T3 Organiser and transmit the locking plan data from the PC to the Palm (see the PalmLDB operating instructions). Insert your Palm Organiser onto the PalmCD2 at an angle and carefully let it snap into place. Start the PalmLDB and test the PalmCD2 (Config-Device → Test).
The PalmCD2 is now ready for operation. To remove the Palm Organiser from the PalmCD2 again, you must press the slide on the back of the PalmCD2 in the direction of the arrow. Then carefully click out the Palm and slide it up.

- The PalmCD2 does not have a low battery warning with firmware versions 9.1 or earlier. If it stops answering or if there are problems with the radio link, check the batteries or replace them. Dispose of used batteries immediately, keep them out of reach of children, do not open them and do not throw them into a fire.

- For firmware version 9.3 and later and PalmLDB 1.26, a battery warning has been implemented. When a battery warning is issued, please change the batteries as soon as possible.

- Avoid direct exposure to the sun and keep the PalmCD2 away from sources of magnetic interference.

3.0 Programming with the PC or Laptop

You can use the cable enclosed with the PalmCD2 to connect it directly to a free COM interface on a PC or laptop. If no COM interface is available, you can optionally acquire a special serial USB converter cable from SimonsVoss. (Only this cable has

been tested and approved by SimonsVoss). In this configuration, you can program all digital components directly on the PC.

If you use the same interface (such as COM1) for both the docking station and the PalmCD2, you need to end the HotSync manager first in order to free the serial interface for the PalmCD2. You can set this up so that it happens automatically by selecting the appropriate settings in the Palm user dialog box. You can also click the symbol in the lower right of the Windows task bar and then click **End**.

☝ You can also match up your personal data with the PalmCD2 by placing your Palm on the PalmCD2, connecting the PalmCD2 to the PC/Laptop and then performing the HotSync process.

4.0 Programming with the Palm Organiser

Create the locking plan with the LDB locking plan software. Program the components on the PC or laptop. When you make changes to the locking plan, the data is transmitted to the Palm Organiser via the docking station (or PalmCD2) so that both computers have the same data stock. Then go to each of the lockings affected by the changes and either read them out or reprogram them from the Palm Organiser with docked PalmCD2. Finally, transmit the new locking system status back to the PC with a new synchronisation process. Refer to the PalmLDB operating instructions for more detailed information.

5.0 Setting Up the PalmCD2 with Transponder Function

You can also use the PalmCD2 as a transponder in your locking system. In this case, the HotSync key functions as the pushbutton. Refer to the chapter on special transponders in the software operating instructions for more details.

6.0 Data Sheet

Battery type	AAA 1.5 V (2x)
Dimensions	120 mm x 70 mm x 20 mm
Degree of protection	IP 20

SmartCD Programming Device

State of : Dezember 2007

Simons Voss technologies

Content

1.0 Safety notes 3
2.0 Introduction 3
3.0 Connecting to a PC/laptop 4
3.1 Charging the batteries 4
4.0 Configuring the Bluetooth connection 5
4.1 First-time installation 5
4.2 Changing the connection 5
5.0 Configuring the USB connection 5
6.0 Start-up 6
7.0 Programming with the SmartCD . . . 6
7.1 . . . in connection with a PC/laptop 6
7.2 . . . in connection with a PDA 6
8.0 Antenna orientation 7
9.0 Replacement of the batteries 8
10.0 Meaning of LED's 9
11.0 Items supplied 9
12.0 Specifications 10

1.0 Safety notes

- Avoid exposure to direct sunlight.
- Keep unit away from sources of magnetic interference.
- Make sure the unit does not drop onto the floor or receive severe shocks of any kind.
- If misused, the lithium batteries installed in the programming unit can pose a risk of fire or burning. Do not open, burn or heat to over 70°C.
- Replace the batteries only with storage batteries approved by SimonsVoss (currently BMZ Li-Ion manganese type US14500V).
- The integrated batteries must be charged for at least 3 hours before first use.
- Dispose of exhausted or non-functioning batteries without delay in accordance with applicable regulations far away from children's reach.
- Faultless programming in conjunction with a Windows Mobile 5.x PDA can only be guaranteed with units approved by SimonsVoss.
- The manufacturer reserves the right to make technical amendments at any time.
- In cases of dispute, the original German manual shall take precedence.

2.0 Introduction

The SmartCD is a programming unit specially designed to be used with a PC/laptop or a Windows Mobile 5.x PDA (Personal Digital Assistant). It allows you to program and retrieve all digital components in the SimonsVoss 3060 system very easily. You can also compare personal data (such as addresses, calendars, etc.) with the PDA.

3.0 Connecting to a PC/laptop

Using the cable supplied, you can connect the SmartCD directly to a PC or laptop via a free USB interface.

All digital components in the SimonsVoss 3060 system can be programmed using a PC/laptop and a SmartCD.

Note: When carrying out programming with a PDA and SmartCD, you must remove the connecting cable from the SmartCD to the PC/laptop. Bluetooth communication between the SmartCD and the PC/laptop is not possible.

Please note: Before connecting the SmartCD to the USB port, ensure that the Bluetooth port is not active. The Bluetooth function will switch off automatically after approx. 15 minutes. It can also be manually deactivated by pressing the button on the programming device. Otherwise communication via the USB port will not be possible.

Transponders can only be programmed when the SmartCD is directly connected to a PC/laptop (by USB cable) and the software program Locking Data Base (LDB) 1.50 or higher or Locking System Management (LSM) 2.2 or higher is installed.

3.1 Charging the batteries

To charge the installed batteries, connect the SmartCD to the PC/laptop using the USB cable. The batteries in the SmartCD are then charged via the USB interface.

Note: The integrated batteries must be charged for at least 3 hours before first use.

Note: In the case of laptops, the USB interface may be deactivated when the laptop is switched off.

Tip: If you do not intend to use the SmartCD for a long period, connect the SmartCD to the USB interface. This will prevent the batteries from running down, and the unit may be used at any time.

Using several devices via a passive external USB hub (without its own power supply) can be problematic. This is because the USB interface cannot supply sufficient power. For this reason, connect the SmartCD directly to a free USB interface on the PC/laptop for charging or use an active USB hub (with its own power supply).

4.0 Configuring the Bluetooth connection

4.1 First-time installation

When coupling the SmartCD and the PDA, ensure that both units are:

- switched on and can be recognised by Bluetooth.
- placed close to one another.

Please refer to the 'SmartLSM' software manual (and the user manual of the PDA manufacturer as necessary) for more information on coupling the SmartCD and PDA.

Select 'SV [*serial number of your unit*]' as the SimonsVoss unit.

When coupling the PDA and SmartCD for the first time, it is important that the reception range does not contain several different SmartCDs with activated Bluetooth.

4.2 Changing the connection

It is possible to change the established Bluetooth connection at any time (in order to perform programming with another SmartCD, for example).

Please refer to the 'SmartLSM' software manual for details of the procedure.

5.0 Configuring the USB connection

When you connect the SmartCD to the PC/laptop using a USB cable for the first time, the Windows operating system will detect new USB hardware. Following the instructions in the installation menu, install the driver contained on the supplied CD onto your desktop computer (selecting the directory 'SmartCD_USB').

If you are working with LDB 1.40a or earlier (or LSM 2.1 or earlier), please note that the new hardware will be installed onto one of the COM interfaces 1-4.

6.0 Start-up

The installed batteries are pre-charged. The unit is therefore ready for immediate use. (Before using the SmartCD for this first time, we recommend charging the unit on a USB port for around 3-4 hours.) To use the programming unit, please perform the following steps:

- Connect the SmartCD to the PC/laptop via USB.
- Install the USB driver for the SmartCD onto the PC/laptop (see supplied CD).

To use the SmartCD with a PDA, perform the following steps in addition:

- Install the SmartLSM locking plan software on the PDA via ActiveSync.
- Couple the SmartCD and PDA using Bluetooth (performed through SmartLSM).
- Set the COM port on the PDA for the SmartCD (performed through SmartLSM)

7.0 Programming with the SmartCD . . .

When programming, note that the minimum distance between the SmartCD and the lock should be 10 cm (30 cm to a Smart Relay and 70 cm to a block lock).

7.1 . . . in connection with a PC/laptop

The latest version of the Locking Data Base (LDB) 1.50a or later, or locking-system-management (LSM) 2.2 or later) software must be installed on the PC/laptop. A programming unit must be connected to the PC/laptop for new installations or software updates.

Note: You will need administrator rights to install the software on Windows NT/2000/XP.

Always carry out a backup before performing an update.

7.2 . . . in connection with a PDA

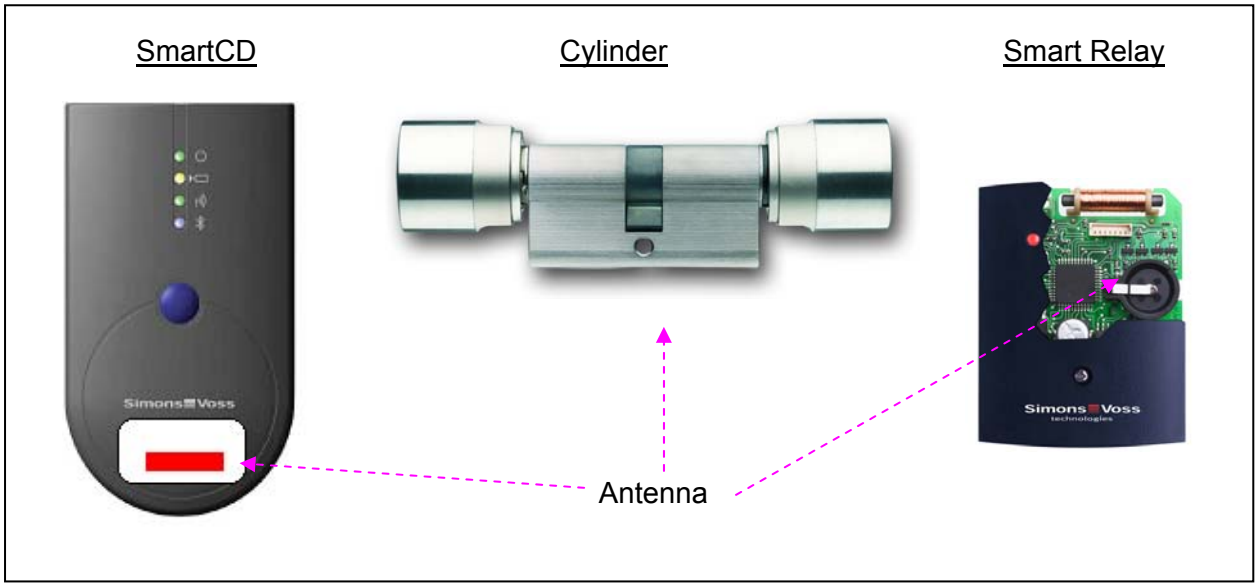
The latest version of LDB must be installed on the PC/laptop. The PDA desktop software must also be set up on the PC/laptop. You must carry out an ActiveSync when installing on the PDA for the first time.

The latest version of SmartLSM must be installed on the PDA using ActiveSync.

You can now transfer a locking plan compiled on the PC/laptop to the PDA by means of ActiveSync. For more details, please refer to the PDA user manual.

8.0 Antenna orientation

The antenna orientation for selected components is shown below to guarantee faultless programming. To ensure the largest possible range when programming, the antennas of the SmartCD and the lock should be aligned parallel to one another. To prevent over-modulation, however, the distance between the antennas should always be at least 10 cm.

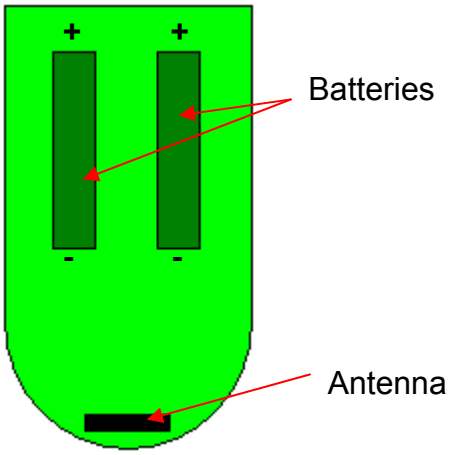


All antennas are aligned parallel to one another in this example.

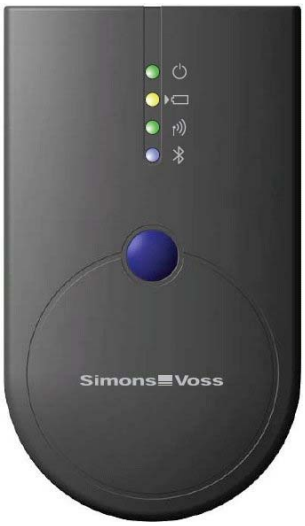
9.0 Replacement of the batteries

Please proceed as follows when you need to change the batteries:

- Remove the belt clip carefully (if you use a small Phillips screwdriver, you do not need to remove the belt clip).
- Remove the screw on the back of the unit.
- Detach the bottom half of the housing.
- Take out the old batteries and insert the new batteries with the positive pole pointing upwards as shown in the diagram. Observe correct polarity and make sure you are using the correct battery type.
- Replace the bottom half of the housing and fasten the screw finger-tight.
- Attach the belt clip.



10.0 Meaning of LED's



First LED (green) on → Unit ready for operation
First LED (green) flashing → Standby

Second LED (yellow) on → Batteries are charging
Second LED (yellow) off → Batteries are charged

Third LED (green) flashing rapidly → Unit is communicating with a SimonsVoss lock
Third LED (green) flashing slowly → No connection to lock

Fourth LED (blue) on → Bluetooth active

The first LED (green) lights when the unit is connected via USB to a PC/laptop, or when the SmartCD is switched on without a USB connection by pressing the button. To save energy, you can switch off the unit by pressing the button again.

The second LED (yellow) only lights when the SmartCD is connected to the computer by USB for charging purposes and at least one of the batteries requires charging.

The third LED (green) only lights when radio communication is established between the SmartCD and a relevant lock (e.g. for programming, retrieval).

The fourth LED (blue) lights when using the Bluetooth interface; it remains lit for the duration of the programming, retrieval or reset procedure and goes out again afterwards.

11.0 Items supplied

SmartCD
Two batteries of type US14500V (installed)
Cable for connecting to a USB interface
CD-ROM containing USB drivers

SimonsVoss LDB software (or SmartLSM for mobile on-site programming) is also needed to use the SmartCD. These are not supplied; they must be purchased separately.

Before start-up, please read the PDA manufacturer manual.

12.0 Specifications

Housing dimensions H x W x D	112 x 63 x 22 mm
Weight (including batteries)	95 g
Housing material	Plastic
Housing colour	Grey
Number of LED's	4
Battery type	Li-Ion manganese storage batteries (rechargeable)
Voltage	4.2 V
Manufacturer	BMZ
Type	US14500V
Number of batteries	2
Protective system	IP20
Working temperature range	–5°C to +40°C
Storage temperature range	–20°C to +60°C
Bluetooth connection	Class 2 transmitting power: 2.5 mW
Profiles supported	SPP Serial Port Profile, serial data transfer

Caption

State of: July 2007

SimonsVoss technologies

Explanation of technical terms

Access logging	Additional function of the digital components in the TC version: The digital lockings store the last 128 accesses with date, time of day and user name. The stored accesses can be read out with the help of the *Config-Device* or PalmCD2 or over the network.
Activation transponder	Can be inserted within the scope of the *shunt lock function*, so that, in case of an emergency, the deactivation of the lockings can be released when the alarm system is activated. The door can then be opened with an authorised transponder.
Activation unit	See *shunt lock function*
Central node	Component of the network installation: is connected to the PC using the RS232 interface and represents the central unit of the *network*.
Deactivation unit	See *shunt lock function*
Higher priority locking level	If a transponder should lock in more than three different locking systems, one sets up a higher priority transponder.
Locking	General term for digital locking cylinders, digital Smart Relays and shunt lock components.
LockNode	Component of the network installation: LockNodes are installed in the vicinity of a digital locking and are connected to the CentralNode over the network wiring. The data transmission from the LockNode to the digital locking takes place over radio without wires. Using the locking plan software, the lockings can be programmed or read out.
Network	All digital components can be connected to a network and configured and administered from a central PC. A physical approach to the lockings with the SmartCD is then no longer necessary.
Overlay mode	Locking systems with up to 1000 transponders can be operated in the so-called overlay mode. If a transponder should be lost in this case, you simply set up a replacement transponder in the locking plan and program it. Then go to all lockings to which this transponder has authorisation. After the activation of the transponder, the locking recognises that this is a replacement transponder. The old, lost transponder is automatically blocked.

SmartCD	The SmartCD is a programming device that was developed especially for wireless operation with a PDA. It makes it very easy to program and read out all digital components of the System 3060. You can also use the PDA to match up your personal data (addresses, calendar, etc.).
Password transponder	Instead of manually entering the password for the locking plan software, you can also transmit it over radio with the password transponder.
Programming transponder	Use the programming transponder to program Digital Locking Cylinder 3061 and Transponder 3064 devices. You do not need a PC or special system software – simply press a button. For example, you can grant or change access authorisation if you lose a key or make changes to the locking plan in small systems.
Repeater (LON)	The repeater (LON) is used to extend the specified cable length of 900 m (984 m) (BUS) in a segment. This requires that an additional LPI10 also be used.
Router (LON)	The router (LON) is used to separate individual segments, such as floors or buildings, for example, from one another in large networks. Likewise, routers are used as intermediary switches in long network lines.
Shunt lock function	Serves the integration of an alarm system into the System 3060. A deactivation unit must be installed on every door that leads to a security area. The activation unit is installed at a central location and connected to the deactivation units. The alarm system can then be activated and deactivated via the activation unit using an authorised transponder. The signals are forwarded to the deactivation units, which prevent a door from being accidentally opened when the alarm system has been activated.
Switching transponder	This transponder has a two-wire cable connected to the switch contacts of the button. This cable is led to the outside of the device.
Time zone control	Additional function of the digital components in the TC Version: Transponders can be programmed such that they are authorised for the lockings only at predetermined times.
Twisted-Pair	Double wire, twisted cable, used for the network cabling.

Special symbols used in the text

☺ Remark, tip

➲ Example

👍 Attention

Subject to technical modifications